

# Matheschülerzirkel Klasse 7/8

Tim Baumann



**Notation.** Wir verwenden die folgenden Bezeichnungen:

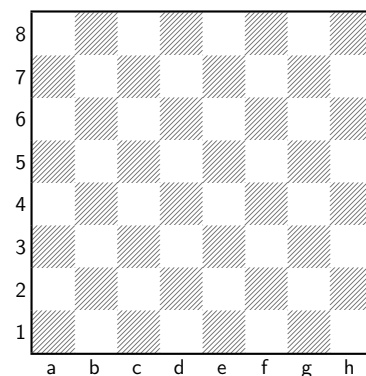
$\mathbb{N}$	Menge der natürlichen Zahlen	$\{1, 2, 3, 4, \dots\}$
$\mathbb{Z}$	Menge der ganzen Zahlen	$\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Q}$	Menge der rationalen Zahlen	$\frac{1}{3}, \frac{-17}{2}, 1 \in \mathbb{Q}$

22. November 2013

## 1 Unmöglichkeitbeweise über Invarianten

Vor uns befindet sich ein leeres Schachbrett und ein großer Haufen Dominosteine. Ein Dominostein ist genauso groß wie zwei Felder des Schachbretts. Wenn du magst, kannst du dir das Schachbrett, die Dominosteine und ein paar Tetris-Steine (die übrigens auch Tetrominos genannt werden), die wir später noch brauchen werden, auf der Zirkel-Webseite<sup>1</sup> ausdrucken, ausschneiden und selbst mitknobeln.

**Frage.** Ist es möglich, das Schachbrett mit Dominosteinen so zu belegen, dass jedes Feld bedeckt ist, keine zwei Dominosteine übereinander liegen und kein Stein über den Rand hinausragt?



<sup>1</sup><http://timbaumann.info/mathezirkel-kurs/invarianten-spiele.html>

*Antwort.* Ja. Lege in jede Zeile des Feldes 4 Dominosteine horizontal nebeneinander.  $\square$

Wir sägen nun aus dem Schachbrett die rechte untere Ecke, das Feld  $h1$ , heraus.

**Frage.** Ist es immer noch möglich, das Schachbrett wie beschrieben mit Dominosteinen zu belegen?

*Antwort.* Nein. Das Schachbrett ohne rechte untere Ecke hat 63 Felder. Jeder Dominostein belegt genau zwei Felder. Wenn eine Überdeckung möglich wäre, so hätte das Schachbrett ohne rechte untere Ecke somit eine gerade Anzahl von Feldern. Also kann es keine Überdeckung geben.  $\square$

Während wir die erste Frage einfach positiv (bejahend) beantworten konnten, indem wir eine Überdeckung mit Dominosteinen angegeben haben, fällt uns die negative (verneinende) Antwort schwieriger: Wir mussten nämlich einen Grund finden, warum es eine solche Überdeckung nicht geben kann. Es reicht nicht aus, zu sagen, man habe keine Lösung gefunden. Es könnte ja immer noch sein, dass man sich nur ungeschickt angestellt hat und deshalb keine Lösung gefunden hat.

Wir sägen nun aus dem Schachbrett auch die linke obere Ecke, das Feld  $h8$ , heraus.

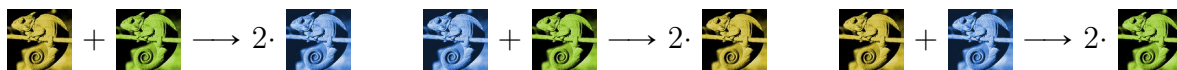
**Frage.** Wie immer: Gibt es nun eine Überdeckung des Schachbretts mit Dominosteinen?

Das Schachbrett ohne die beiden Ecken hat wieder eine gerade Anzahl von Feldern, nämlich 62. Prinzipiell könnte also eine Überdeckung möglich sein. Aber wenn du versuchst, eine zu finden, wirst du feststellen dass, egal wie du dich anstellst, zwei Felder übrig bleiben. Du vermutest daher, dass es keine Lösung geben kann.

*Antwort.* Nein. Wenn man einen Dominostein auf das Brett legt, so bedeckt er, egal wie er liegt, ein weißes und ein schwarzes Feld. Die beiden Felder, die wir abgesägt haben, waren beides weiße Felder. Damit ist das um zwei Ecken verkleinerte Brett noch 30 weiße und 32 schwarze Felder. Jedes Mal, wenn wir einen Stein setzen, nimmt die Zahl der noch offenen weißen und die Zahl der noch offenen schwarzen Felder um je 1 ab. Nach drei gelegten Dominosteinen haben wir beispielsweise noch  $30 - 3 = 27$  offene weiße und  $32 - 3 = 29$  offene schwarze Felder. Zu jedem Zeitpunkt gibt es genau zwei schwarze unbedeckte Felder mehr als weiße unbedeckte Felder. Wenn alle weißen Felder bedeckt sind, gibt es also noch zwei schwarze offene Felder. Diese können aber nicht nebeneinander liegen, deshalb können sie nicht mit einem Domino überdeckt werden.  $\square$

Wären nicht zwei diagonal gegenüberliegende, sondern zwei Ecken, die an einer Seite liegen, herausgesägt worden, so wäre die Aufgabe lösbar gewesen. Bevor wir die Antwort etwas tiefer analysieren, wollen wir uns noch eine weitere Aufgabe anschauen:

**Aufgabe.** Auf einer Insel leben 345 gelbe, 346 grüne und 347 blaue Chamäleons. Wann immer sich zwei Chamäleons gleicher Farbe begegnen, passiert nichts. Wenn sich aber zwei Chamäleons unterschiedlicher Farbe begegnen, so nehmen beide die dritte Farbe an. Beispielsweise hätten wir nach einem Treffen eines gelben und einer grünen Chamäleons nur noch 344 gelbe, 345 grüne, aber dafür 349 blaue Chamäleons. Frage: Ist es möglich, dass zu einem Zeitpunkt genau gleich viele Chamäleons jeder Farbe auf der Insel leben?



Grundsätzlich könnte diese Situation eintreten, da  $345 + 346 + 347 = 1038$  durch 3 teilbar ist. Wenn wir allerdings versuchen, eine Liste von Begegnungen zu erstellen, sodass nach diesen Begegnungen die Anzahl der Chamäleons jeder Farbe gleich ist, scheitern wir. Spoiler: Auch diese Aufgabe ist nicht lösbar.

Was haben diese Aufgaben gemeinsam? Zunächst haben wir eine Anfangssituation, beispielsweise das leere (verkleinerte) Schachbrett oder die Anzahlen der Fische jeder Farbe im Aquarium. Dann verändert sich die Ausgangslage durch Züge (das Legen eines Dominosteins) oder Ereignisse (Treffen von zwei Fischen). Die Frage in beiden Aufgaben ist, ob eine bestimmte Situation (alle Felder bedeckt bzw. gleich viele Fische von jeder Farbe) eintreten kann.

In beiden Aufgaben finden wir experimentell keine Lösung und suchen daher nach einem Grund, warum wir jedes solche Unterfangen von vornherein zum Scheitern verurteilt ist. In der Schachbrettaufgabe könnten wir dies begründen, indem wir alle Möglichkeiten ausprobieren. Davon gibt es allerdings ziemlich viele, sodass wir eine Antwort auf diesem Weg nur, wenn überhaupt, mit Hilfe eines Computers finden können. In der zweiten Aufgabe allerdings, gibt es (auf den ersten Blick) unendlich viele Möglichkeiten, wie sich Fische treffen können; wenn wir beispielsweise herausgefunden haben, dass wir mit 40 Treffen von Fischen die gewünschte Endsituation nicht erreichen können, so könnte uns das 41 Treffen zum Ziel führen.

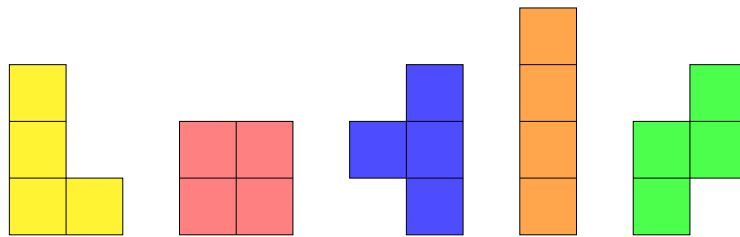
Wir haben uns daher in der Aufgabe mit dem Schachbrett eines anderen Tricks bedient: Wir haben bemerkt, dass am Anfang das verkleinerte Brett  $32 - 30 = 2$  schwarze Felder mehr besitzt als weiße Felder. Jedes Mal, wenn wir einen Dominostein gelegt haben, wurde ein weißes und ein schwarzes Feld verdeckt, also blieb die Differenz zwischen der Anzahlen der schwarzen offenen und weißen offenen Felder immer gleich. Wir haben also eine Zahl entdeckt, die wir für jedes unbedeckte, teilweise oder vollständig mit Steinen bedeckte Spielbrett ausrechnen können und die mit jedem weiteren platzierten Stein, egal wo er gelegt wird, gleich bleibt. Man sagt auch, dass diese Zahl unverändert (mit Fremdwort *invariant*) bleibt und nennt sie eine *Invariante*. In der gewünschten Endposition, dass das ganze Brett belegt ist, wäre die Differenz zwischen den offenen schwarzen und offenen weißen Feldern gleich  $0 - 0 = 0$ . Diese Situation kann also beginnend bei unserer Anfangsposition nicht erreicht werden.

*Antwort.* Es ist nicht möglich, dass es irgendwann gleich viele Chamäleons von jeder Farbe gibt. Wir betrachten die Zahl  $C$ , die wir als Differenz zwischen der Anzahl der blauen und grünen Chamäleons festlegen. Zu Beginn ist  $C = 347 - 346 = 1$ . Wenn sich ein blaues und ein grünes Chamäleon treffen, so bleibt diese Zahl gleich. Wenn sich allerdings ein grünes und ein gelbes Chamäleon treffen, so nimmt die Zahl der grünen Chamäleons um eins ab, während die Zahl der blauen um zwei steigt. Insgesamt erhöht sich  $C$  um drei. Wenn sich ein blaues und ein gelbes Chamäleon treffen, so sinkt  $C$  um drei (mit ähnlicher Begründung). Die Zahl  $C$  ist also nicht invariant. Aber wir stellen fest: Zu Beginn ist  $C$  gleich 1, also nicht durch 3 teilbar. Wir wissen aber: Wenn eine ganze Zahl  $k \in \mathbb{Z}$  durch 3 teilbar ist, so sind auch die Zahlen  $k + 3$  und  $k - 3$  durch 3 teilbar. Umgekehrt ist, wenn  $k \in \mathbb{Z}$  nicht durch 3 teilbar ist, auch die Zahlen  $k + 3$  und  $k - 3$  nicht durch 3 teilbar. Also können wir folgern, dass nach jedem Treffen von zwei Chamäleons unsere Zahl immer noch *nicht* durch 3 teilbar ist. Unsere Invariante ist hier also nicht die Zahl  $C$  selbst, sondern die Tatsache, dass  $C$  nicht durch 3 teilbar ist. In der gewünschten Endsituation wäre  $C = 0$ , da wir verlangen, dass die Zahl der blauen und grünen Chamäleons dann gleich ist. Aber 0 ist durch 3 teilbar! Folglich kann diese Situation nicht erreicht werden.  $\square$

Invarianten sind ein nützliches Mittel für Aufgaben obiger Art, bei denen man zeigen soll, dass eine bestimmte Situation nicht erreicht werden kann. Ein Nachteil dieser Technik ist es,

dass Invarianten oft nicht offensichtlich sind, sondern es einiger Kreativität und Erfahrung bedarf, um sie zu finden. Bei der Schachbrettaufgabe könnte man feststellen, dass am Ende jedes Versuches zwei schwarze Felder übrig bleiben. Generell bietet sich an, wenn man so eine Aufgabe angeht, erst einmal rumzuprobieren und dabei Zahlen, die einem wichtig erscheinen, nach jedem Schritt aufzuschreiben und danach nach Mustern zu suchen.

Auch in der höheren Mathematik spielen Invarianten eine wichtige Rolle: Es gibt beispielsweise eine Teilgebiet der Mathematik, das sich mit Knoten befasst. Einen Knoten stellt man sich dabei als Seil im dreidimensionalen Raum vor, wobei Anfang und Ende des Seils zusammengebunden sind. Wenn wir einen Knoten haben, so stellen sich Mathematiker die Frage, ob wir diesen Knoten nur durch Bewegen des Seiles (ohne Zerschneiden) diesen Knoten auflösen können, sodass er nur noch aus einer einfachen Seilschlinge besteht. Um zu beweisen, dass dies für manche Knoten nicht möglich ist, haben Mathematiker Invarianten gefunden, die etwas komplizierter als unsere bisher gesehene Invarianten sind und beim Umformen eines Knoten gleich bleiben.

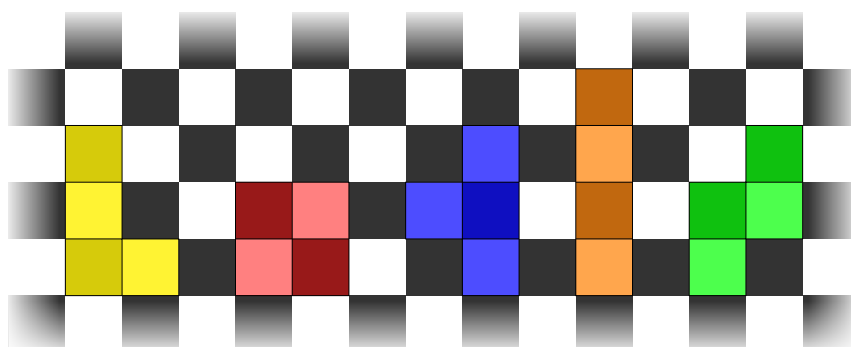


Oben siehst du die fünf verschiedenen Formen, die beim Spiel Tetris auftreten.

**Frage.** Ist es möglich, aus den obigen fünf Figuren ein Rechteck zu legen? Dabei dürfen sich die Figuren nicht überlappen, aber beliebig oft gedreht oder gespiegelt werden.

Zunächst einmal stellen wir fest, dass die fünf Figuren insgesamt  $5 \cdot 4 = 20$  Felder belegen. Also muss das Rechteck, falls es existiert, entweder 1 Feld breit und 20 Felder lang oder 2 Felder breit und 10 Felder lang oder 4 Felder breit und 5 Felder lang sein. Offensichtlich scheidet die erste Möglichkeit aus. Man kann sich auch recht schnell überlegen, dass auch die zweite Möglichkeit nicht in Frage kommt (Tipp: platziere das orange Teil zuerst). Somit bleibt nur das  $5 \times 4$ -Rechteck als Möglichkeit übrig. Wenn wir aber versuchen, solch ein Rechteck mit obigen Figuren zu belegen, scheitern wir immer wieder. Das hat auch einen Grund:

*Antwort.* Es ist nicht möglich, aus den Tetris-Figuren ein Rechteck zu legen. Wir legen die Figuren auf ein Schachbrett:



Nun fällt etwas auf: Alle Figuren bis auf die blaue belegen je zwei weiße und zwei schwarze Felder (egal, wie man sie hinlegt). Die blaue Figur, jedoch, belegt drei weiße Felder und nur ein schwarzes Feld (oder umgekehrt). Damit belegen die Figuren zusammengenommen ungleich viele weiße wie schwarze Felder, egal wie man sie anordnet. Damit kann man insbesondere kein  $4 \times 5$ -Rechteck mit ihnen legen, denn jedes  $4 \times 5$ -Rechteck auf einem Schachfeld hat gleich viele weiße und schwarze Felder.  $\square$

6. und 20. Dezember 2013, 10. Januar 2014

## 2 Rechnen mit Restklassen

### 2.1 Teilbarkeit

**Definition 1.** Eine Zahl  $b \in \mathbb{Z}$  ist durch  $a \in \mathbb{Z}$  *teilbar*, wenn es eine Zahl  $c \in \mathbb{Z}$  gibt mit

$$a \cdot c = b.$$

**Notation.** Wir verwenden dann die Kurzschreibweise  $a \mid b$ , gesprochen „ $a$  teilt  $b$ “. Wir sagen auch, dass  $a$  ein *Teiler* von  $b$  ist oder dass  $b$  ein Vielfaches von  $a$  ist. Im Fall, dass die Zahl  $a$  die Zahl  $b$  *nicht* teilt, d. h. keine Zahl  $c \in \mathbb{Z}$  existiert mit  $a \cdot c = b$ , schreiben wir  $a \nmid b$ .

**Beispiel.** Folgende Aussagen stimmen:

- $3 \mid 6$
- $5 \nmid 13$
- $8 \mid -8$
- $3 \mid 12345$
- $2 \nmid 1001$

**Exkurs.** Der Ausdruck  $a \mid b$  ist eine mathematische Aussage. Andere Beispiele für mathematische Aussagen sind:

- $\sqrt{2}$  ist irrational
- $3 > 5$
- $n$  ist gerade
- $m$  ist eine Primzahl
- Jeder Winkel lässt sich mit Zirkel und Lineal halbieren.
- Für  $n \in \mathbb{N}$  mit  $n \geq 2$  gibt keine Zahlen  $a, b, c \in \mathbb{N}$ , sodass  $a^n + b^n = c^n$  stimmt.
- Es gibt unendlich viele Primzahlenszwillinge, das sind Primzahlen  $p$  und  $q$ , mit  $q = p + 2$ .

Mathematische Aussagen können richtig oder falsch sein. Beispielsweise ist in den obigen Beispielen die erste wahr, die zweite falsch und über die nächsten beiden können wir nichts sagen, da sie Zahlen  $n$  und  $m$  beinhalten, die erst noch genauer definiert werden müssen. Die vorletzte Aussage trägt den Namen „Fermats letzter Satz“ und ist richtig, doch hat es über 300 Jahre gedauert, bis sie bewiesen werden konnte. Von der letzten Aussage wird vermutet, dass sie stimmt, es existiert jedoch kein Beweis.

**Frage.** Gibt es eine Zahl  $a \in \mathbb{Z}$ , die Teiler von 0 ist, d. h.  $a \mid 0$ ?

*Antwort.* Ja, wir können sogar jede beliebige Zahl  $a \in \mathbb{Z}$  nehmen: Setze  $c := 0$ , dann ist  $a \cdot c = a \cdot 0 = 0$  und somit ist die Definition erfüllt.  $\square$

**Frage.** Gibt es andersherum eine Zahl  $b \in \mathbb{Z}$ , die durch 0 teilbar ist, also  $0 \mid b$ ?

*Antwort.* Ja, aber nur die Zahl 0 selber. Mit  $a = 0$ , ist für ein beliebiges  $c$  nämlich  $a \cdot c = 0 \cdot c = 0$ , also muss  $b = 0$  sein.  $\square$

**Exkurs.** Sei  $z \in \mathbb{Z}$  eine ganze Zahl. Wenn  $z$  ungerade ist, so ist  $z$  nicht durch 8 teilbar. Um nicht immer „wenn ..., dann ...“ schreiben zu müssen, verwenden Mathematiker folgende Notation:

$$z \text{ ist ungerade} \implies 8 \nmid z$$

Dabei stehen auf der linken und rechten Seite des  $\implies$ -Zeichens mathematische Aussagen  $P$  und  $Q$ . Die Zeile  $(P \implies Q)$  ist wiederum selbst eine mathematische Aussage, nämlich die Aussage, dass wenn  $P$  stimmt, dann auch  $Q$  stimmt. Dabei ist es wichtig, dass links  $P$  steht und rechts  $Q$ , denn in unserem Beispiel stimmt die Aussage andersrum nicht: Wenn  $z$  nicht durch 8 teilbar ist, dann muss  $z$  noch nicht unbedingt ungerade sein. Zum Beispiel ist  $z = 4$  nicht durch 8 teilbar, aber gerade.

Ein anderes Beispiel: Eine ganze Zahl  $m$  ist ungerade, wenn die Zahl  $(m+1)$  gerade ist. Andersrum ist  $(m+1)$  gerade, wenn  $m$  ungerade ist. Hier ist also die Umkehrung erfüllt, im Gegensatz zum vorherigen Beispiel. Also ist  $m$  immer dann und nur dann ungerade, wenn  $(m+1)$  ungerade ist. Mathematiker verwenden dafür eine besondere Notation:

$$n \text{ ist ungerade} \iff (n+1) \text{ ist gerade}$$

Auf beiden Seiten des  $\iff$ -Zeichens stehen dabei wieder mathematische Aussagen. Der Pfeil  $\iff$  bedeutet, dass die linke Aussage nur dann stimmt, wenn die rechte Aussage stimmt.

Wir wollen nun ein paar Tatsachen über die Teilbarkeit beweisen.

**Behauptung 1.** Seien  $n, p, q \in \mathbb{Z}$  ganze Zahlen. Dann gilt:

- (i)  $n \mid p$  und  $p \mid q \implies n \mid q$
- (ii)  $n \mid p \implies n \mid (p \cdot q)$
- (iii)  $n \mid p$  und  $n \mid q \implies n \mid (p + q)$

*Beweis.* Zu (i): Aus der Definition von Teilbarkeit wissen wir, dass es  $c, d \in \mathbb{Z}$  gibt mit

$$n \cdot c = p \quad \text{und} \quad p \cdot d = q$$

Um zu zeigen, dass  $n \mid q$  gilt, müssen wir nach derselben Definition eine Zahl für die Leerstelle finden, sodass die Gleichung

$$n \cdot \_\_ = q$$

erfüllt ist. Wir behaupten, dass die Zahl  $p := (c \cdot d)$  dies leistet. Wir rechnen nämlich nach:

$$n \cdot (c \cdot d) = \underbrace{(n \cdot c)}_{=p} \cdot d = p \cdot d = q.$$

Dabei haben wir im ersten Schritt das Assoziativgesetz gebraucht.

Zu (ii): Aus der Definition von Teilbarkeit erhalten wir ein  $c \in \mathbb{Z}$  mit

$$n \cdot c = p.$$

Wir müssen folgende Leerstelle sinnvoll ersetzen:

$$n \cdot \_\_ = p \cdot q.$$

Wir nehmen dafür die Zahl  $(c \cdot q)$  und rechnen

$$n \cdot (c \cdot q) = \underbrace{(n \cdot c)}_{=p} \cdot q = p \cdot q$$

Zu (iii): Aus der Definition erhalten wir  $c, d \in \mathbb{Z}$  mit

$$n \cdot c = p \quad \text{und} \quad n \cdot d = q.$$

Es soll folgende Gleichung gelten:

$$n \cdot \_\_ = p + q$$

Wir setzen  $(c + d)$  für  $\_\_$  und rechnen

$$n \cdot (c + d) = \underbrace{n \cdot c}_{=p} + \underbrace{n \cdot d}_{=q} = p + q.$$

Im ersten Schritt haben wir dabei das Distributivgesetz angewendet.

□

**Achtung.** Folgendes Rechengesetz gilt *nicht*:

$$p \mid n \text{ und } q \mid n \implies (p \cdot q) \mid n$$

Ein Gegenbeispiel dafür ist  $p = 4, q = 6, n = 12$ .

**Exkurs.** In den natürlichen Zahlen  $\mathbb{N}$ , den ganzen Zahlen  $\mathbb{Z}$  und den rationalen Zahlen  $\mathbb{Q}$  gelten folgende Rechenregeln:

- *Kommutativgesetz*:  $a + b = b + a$  und  $a \cdot b = b \cdot a$
- *Assoziativgesetz*:  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- *Distributivgesetz*:  $a \cdot (b + c) = a \cdot b + a \cdot c$

Es ist eine gute Übung, sich zu überlegen, welche Plus- und Mal-Zeichen wir durch Minus- und Divisions-Zeichen ersetzen dürfen, sodass die Regeln immer noch stimmen.

## 2.2 Restklassen

Übungszettel vom 10. Januar 2014: <http://timbaumann.info/mathezirkel-kurs/uebung4.pdf>

Sei  $n$  eine natürliche Zahl und  $p, q$  natürliche Zahlen, die bei der Division durch  $n$  den gleichen Rest  $r$  haben, also

$$p : n = a \text{ Rest } r$$

$$q : n = b \text{ Rest } r$$

für zwei Zahlen  $a, b \in \mathbb{Z}$ . Wir können dabei außerdem annehmen, dass  $r$  eine Zahl zwischen 0 bis  $n - 1$  ist (warum?). Wenn wir obige Gleichungen umschreiben, erhalten wir

$$p = n \cdot a + r,$$

$$q = n \cdot b + r.$$

Wir rechnen:

$$p - q = (n \cdot a + r) - (n \cdot b + r) = n \cdot a + r - n \cdot b - r = n \cdot a + n \cdot b = n \cdot (a + b).$$

Wir haben also  $n \cdot (a + b) = p - q$ , folglich nach Definition von Teilbarkeit  $n \mid (p - q)$ . Dies ist unser erstes halbwegs interessantes Ergebnis: Zwei Zahlen  $p$  und  $q$ , die bei Division durch  $n$  den gleichen Rest haben, unterscheiden sich nur durch ein Vielfaches von  $n$ .

**Definition 2.** Für zwei Zahlen  $p$  und  $q$ , die sich nur durch ein Vielfaches von  $n \in \mathbb{N}$  unterscheiden (d. h.  $n \mid (p - q)$ ) schreiben wir

$$p \equiv q \pmod{n}.$$

Wir sprechen: „ $p$  ist gleich  $q$  modulo  $n$ “.

**Notation.** Falls  $p \equiv q \pmod{n}$  nicht stimmt, schreiben wir  $p \not\equiv q \pmod{n}$ .

**Beispiel.** Folgende Aussagen stimmen:

- $1 \equiv 4 \pmod{3}$
- $-4 \equiv 3 \pmod{7}$
- $4 \not\equiv 2 \pmod{4}$
- $0 \equiv 16 \pmod{8}$
- $-1001 \equiv -1003 \pmod{2}$
- $0 \not\equiv -101 \pmod{3}$

**Achtung.** Wir dürfen den Teil in Klammern auf keinen Fall weglassen! Es gilt nämlich  $4 \equiv 7 \pmod{3}$ , aber nicht  $4 \equiv 7 \pmod{6}$ !

**Behauptung 2.** Sei  $n \in \mathbb{N}$  und  $a, a_1, a_2, b, b_1, b_2, c \in \mathbb{Z}$  ganze Zahlen. Dann gilt:

- (i)  $a \equiv a \pmod{n}$
- (ii)  $a \equiv b \pmod{n}$  und  $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$
- (iii)  $a_1 \equiv a_2 \pmod{n}$  und  $b_1 \equiv b_2 \pmod{n} \implies a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$
- (iv)  $a_1 \equiv a_2 \pmod{n}$  und  $b_1 \equiv b_2 \pmod{n} \implies a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}$



*Beweis.* Zu (i): Es ist  $a - a = 0$  und somit gilt  $n \mid (a - a)$ , da 0 von jeder beliebigen Zahl geteilt wird.

Zu (ii): Es gilt nach Voraussetzung  $n \mid (a - b)$  und  $n \mid (b - c)$ , also nach unserem Wissen über Teilbarkeit

$$n \mid \underbrace{((a - b) + (b - c))}_{=(a-c)}.$$

Zu (iii): Nach Voraussetzung gilt  $n \mid (a_1 - a_2)$  und  $n \mid (b_1 - b_2)$ . Somit

$$n \mid \underbrace{((a_1 - a_2) - (b_1 - b_2))}_{=(a_1+b_1)-(a_2+b_2)}.$$

Zu (iv): Nach Voraussetzung gilt  $n \mid (a_1 - a_2)$  und  $n \mid (b_1 - b_2)$ . Somit gilt auch

$$n \mid (a_1 - a_2) \cdot b_1 \quad \text{und} \quad n \mid a_2 \cdot (b_1 - b_2),$$

also auch  $n \mid ((a_1 - a_2) \cdot b_1 + a_2 \cdot (b_1 - b_2))$ . Es gilt aber

$$(a_1 - a_2) \cdot b_1 + a_2 \cdot (b_1 - b_2) = a_1 \cdot b_1 - a_2 \cdot b_1 + a_2 \cdot b_1 - a_2 \cdot b_2 = a_1 \cdot b_1 - a_2 \cdot b_2,$$

somit ist dies gleichbedeutend zu  $n \mid (a_1 \cdot b_1 - a_2 \cdot b_2)$ .  $\square$

**Definition 3.** Sei  $n \in \mathbb{N}$  eine natürliche und  $a \in \mathbb{Z}$  eine ganze Zahl. Die *Restklasse* von  $a$  modulo  $n$  ist nun die Menge aller Zahlen, die gleich  $a$  modulo  $n$  sind, also

$$\bar{a} := \{z \in \mathbb{Z} \mid z \equiv a \pmod{n}\}.$$

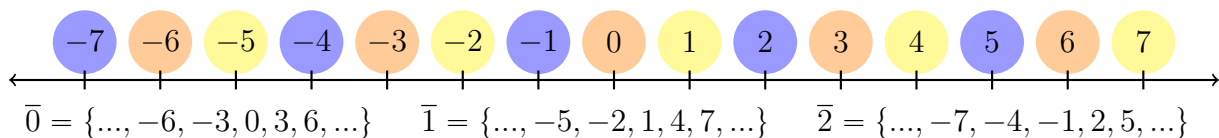
**Notation.** Obige Notation bedeutet: Die Menge aller Zahlen  $z \in \mathbb{Z}$ , die die Bedingung rechts neben dem Mittelstrich erfüllen, also  $z \equiv a \pmod{n}$ .

**Aufgabe.** Überzeuge dich davon, dass gilt:

$$\bar{a} = \{\dots, a + (-3) \cdot n, a + (-2) \cdot n, a + (-1) \cdot n, a, a + 1 \cdot n, a + 2 \cdot n, a + 3 \cdot n, \dots\}.$$

Folgere, dass es genau  $n$  verschiedene Restklassen modulo  $n$  gibt und dass jede ganze Zahl in genau einer Restklasse enthalten ist.

**Beispiel.** Auf dem Zahlenstrahl unten sind alle Zahlen in einer Restklasse modulo 3 in der gleichen Farbe hinterlegt:



Mit Restklassen können wir auch die Chamäleons-Aufgabe genauer analysieren: In der Lösung dieser Aufgabe haben wir  $C$  als die Differenz zwischen der Anzahl der blauen und grünen Chamäleons festgelegt. Zu Beginn ist diese  $C = 347 - 346 = 1$ . Wir haben festgestellt, dass diese Zahl bei jeder Begegnung von Chamäleons gleichbleibt, um drei steigt oder um drei sinkt. Also verlässt diese Zahl die Restklasse der Zahl 1 modulo 3 nicht. Insbesondere wird  $C$  niemals den Wert 0 annehmen, da dieser nicht in der Restklasse der Zahl 1 modulo 3 enthalten ist.

**Behauptung 3.** Für alle  $n \in \mathbb{N}$  gilt

$$10^n \equiv \underbrace{1\,00\cdots 0}_{n \text{ Nullen}} \equiv 1 \pmod{3}$$

*Beweis.* Es gilt

$$\underbrace{99\cdots 9}_{n \text{ Neuner}} = 3 \cdot \underbrace{33\cdots 3}_{n \text{ Dreier}},$$

also  $3 \mid 99\cdots 9$  bzw.  $99\cdots 9 \equiv 0 \pmod{3}$ . Wir rechnen:

$$10^n \equiv \underbrace{99\cdots 9}_{n \text{ Neuner}} + 1 \equiv 0 + 1 \equiv 1 \pmod{3}. \quad \square$$

Du kennst wahrscheinlich folgenden Test auf Teilbarkeit durch 3: Er besagt, dass eine Zahl genau dann durch 3 teilbar ist, wenn ihre Quersumme durch 3 teilbar ist. Vielleicht hast du dich auch schon einmal gefragt, warum dieser Test funktioniert. Mit der Vorarbeit, die wir bisher geleistet haben, fällt ein Beweis nicht schwer:

**Behauptung 4.** Sei  $a \in \mathbb{Z}$  eine ganze Zahl, wobei die Ziffern von  $a$  im Zehnersystem  $a_n, \dots, a_0$  seien, also  $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0$ . Die Quersumme von  $a$  ist dann gegeben durch  $QS(a) = a_n + a_{n-1} + \dots + a_1 + a_0$ . Es gilt dann

$$a \equiv QS(a) \pmod{3}.$$

*Beweis.* Es gilt für alle  $i$  zwischen 0 und  $n$

$$a_i \cdot 10^i \equiv a_i \cdot 1 \equiv a_i \pmod{3}$$

durch Anwenden der letzten Behauptung und den Modulo-Rechenregeln. Also haben wir

$$a \equiv a_n \cdot 10^n + \dots + a_1 \cdot 10 + a_0 \equiv a_n + \dots + a_1 + a_0 \equiv QS(a) \pmod{3}. \quad \square$$

Das ist nicht ganz die Behauptung des Quersummentests, allerdings ist  $m \in \mathbb{Z}$  genau dann durch 3 teilbar, wenn  $m \equiv 0 \pmod{3}$ . Falls aber  $QS(a)$  durch 3 teilbar ist, so haben wir  $QS(a) \equiv 0$  und es folgt mit der ersten Modulo-Rechenregel schon

$$a \equiv QS(a) \equiv 0 \pmod{3}.$$

In beiden obigen Behauptungen kann man auch die Zahl 3 durch die Zahl 9 ersetzen, ohne dass dadurch die Behauptungen falsch werden (gehe die Beweise durch und überlege dir, warum das möglich ist). Somit erhalten wir einen Test auf Teilbarkeit durch 9: Eine Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.

Es gibt auch einen ganz ähnlichen Test für Teilbarkeit durch 11: Eine Zahl  $a \in \mathbb{Z}$  ist genau dann durch 11 teilbar, wenn die alternierende Quersumme durch 11 teilbar ist. Sei  $a = a_n \cdot 10^n + \dots + a_1 \cdot 10 + a_0$ , dann ist die alternierende Quersumme von  $a$

$$\text{AQS}(a) = a_0 - a_1 + a_2 - a_3 + \dots \pm a_n.$$

Wenn  $n$  gerade ist, steht dabei ein Plus-Zeichen vor  $a_n$ , sonst ein Minuszeichen. Das Wort alternierend deutet an, dass wir abwechselnd die Ziffern, beginnend bei der letzten, dazuzählen und abziehen.

Zum Beispiel ist  $\text{AQS}(1234321) = 1 - 2 + 3 - 4 + 3 - 2 + 1 = 0$  und da 0 durch 11 teilbar ist, ist auch 1234321 durch 11 teilbar.

Wir wollen nun beweisen, dass dieser Teilbarkeitstest immer richtig funktioniert. Dazu zunächst eine Vorüberlegung:

**Behauptung 5.** Für alle  $n \in \mathbb{N}$  gilt

$$10^n \equiv \underbrace{1 \underbrace{00 \dots 0}_{n \text{ Nullen}}}_{\substack{\underbrace{\phantom{00 \dots 0}}_{n \text{ Nullen}}} \equiv \begin{cases} 10 \equiv -1, & \text{falls } n \text{ ungerade} \\ 1, & \text{falls } n \text{ gerade} \end{cases} \pmod{11}$$

*Beweis.* Zunächst einmal gilt, wie man leicht nachrechnet,  $100 \equiv 1 \pmod{11}$  und  $10 \equiv -1 \pmod{11}$ . Die Behauptung stimmt also schon mal für  $n=1$  und  $n=2$ . Für beliebige gerade  $n$  folgt nun:

$$10^n \equiv 100^{\frac{n}{2}} \equiv \underbrace{100 \cdot 100 \cdot \dots \cdot 100}_{\frac{n}{2} \text{ Hunderter}} \equiv 1 \cdot 1 \cdot \dots \cdot 1 \equiv 1 \pmod{11}.$$

Für ungerade Zahlen  $n$  rechnen wir analog:

$$10^n \equiv 10 \cdot 100^{\frac{n-1}{2}} \equiv 10 \cdot \underbrace{100 \cdot 100 \cdot \dots \cdot 100}_{\frac{n-1}{2} \text{ Hunderter}} \equiv 10 \cdot 1 \cdot 1 \cdot \dots \cdot 1 \equiv 10 \equiv -1 \pmod{11}. \quad \square$$

**Behauptung 6.** Sei  $a \in \mathbb{Z}$  eine ganze Zahl, wobei die Ziffern von  $a$  im Zehnersystem  $a_n, \dots, a_0$  seien, also  $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0$ . Dann gilt:

$$a \equiv \text{AQS}(a) \pmod{11}.$$

*Beweis.* Es gilt für alle  $i$  zwischen 0 und  $n$

$$a_i \cdot 10^i \equiv \begin{cases} a_i \cdot (-1) \equiv -a_i, & \text{falls } i \text{ ungerade} \\ a_i \cdot 1 \equiv a_i, & \text{falls } i \text{ gerade} \end{cases} \pmod{11}$$

durch Anwenden der letzten Behauptung und den Modulo-Rechenregeln. Also haben wir

$$a \equiv a_0 + a_1 \cdot 10 + \dots + a_n \cdot 10^n \equiv a_0 - a_1 + \dots \mp a_{n-1} \pm a_n \equiv \text{AQS}(a) \pmod{11},$$

wobei  $a_n$  addiert wird, falls  $n$  gerade ist, sonst subtrahiert.  $\square$

Inbesondere folgt: Die Zahl  $a$  ist genau dann durch 11 teilbar (also  $a \equiv 0 \pmod{11}$ ), wenn  $\text{AQS}(a)$  durch 11 teilbar ist (also  $\text{AQS}(a) \equiv 0 \pmod{11}$ ).

24. Januar 2014

### 3 Nim-Spiele

Folgendes Spiel könnte dir bekannt vorkommen:

Auf einem Haufen liegt eine Anzahl von Steinen. Zwei Spieler sind abwechselnd an der Reihe und dürfen in jedem Zug einen, zwei oder drei Steine vom Haufen nehmen. Verloren hat derjenige Spieler, für den keine Steine mehr übrig sind (also hat der Spieler gewonnen, der den letzten Stein vom Haufen nimmt).

Betrachten wir folgende Spielsituation: Auf dem Haufen liegen noch genau vier Steine und dein Gegner ist an der Reihe. Er kann in diesem Zug nicht gewinnen, da er maximal drei Steine vom Haufen nehmen darfst. Nach seinem Zug allerdings werden nur noch ein, zwei oder drei Steine auf dem Haufen sein, je nachdem, ob er in diesem Zug drei, zwei oder einen Stein nimmt. Diese restlichen Steine kannst du in deinem nächsten Zug nehmen und hast gewonnen.

Also solltest du versuchen, dafür zu sorgen, dass nach einem deiner Züge genau vier Steine auf dem Haufen liegen. Dann hast du automatisch gewonnen. Wie können wir dieses Ziel erreichen? Dafür betrachten wir eine weitere Spielsituation:

Auf dem Steinhaufen liegen genau acht Steine. Dein Gegner ist an der Reihe. Nach seinem Zug liegen entweder fünf, sechs oder sieben Steine auf dem Haufen. Du kannst dann einen, zwei bzw. drei Steine nehmen, sodass nach deinem Zug noch genau vier Steine auf dem Haufen liegen. Damit hast du gewonnen.

Wenn nun auf dem Haufen zwölf Steine liegen und dein Gegner an der Reihe ist, dann kannst du dafür sorgen, dass nach seinem und deinem Zug acht Steine auf dem Haufen sind.

Allgemeiner hast du eine Strategie zu gewinnen, wenn dein Gegner an der Reihe ist und die Anzahl der Steine ein Vielfaches von vier ist, bzw. du an der Reihe bist und die Anzahl an Steinen kein Vielfaches von vier ist. Du musst dabei einfach, wenn du an der Reihe bist, so viele Steine nehmen, sodass die Anzahl auf dem Haufen ein Vielfaches von vier ist.

**Aufgabe.** Spiele dieses Spiel gegen deine Freunde/Eltern/Geschwister und beobachte, wie lang sie brauchen, bis sie die Strategie verstanden haben.

Wir wollen nun ein ähnliches Spiel analysieren:

Auf dem Tisch liegen mehrere Steinhaufen. Wir zuvor sind die beiden Spieler abwechselnd an der Reihe. Sie suchen sich in jedem Zug einen Steinhaufen aus. Dann dürfen sie von diesem (und nur von diesem Haufen) eine beliebige Anzahl von Steinen nehmen. Dabei müssen sie mindestens einen und können maximal alle Steine dieses Haufens nehmen. Wie im vorherigen Spiel hat derjenige Spieler verloren, der keinen Zug mehr machen kann.

Für dieses Spiel gibt es ebenfalls eine Gewinnstrategie. Diese benötigt sogenannte Binärzahlen:

**Exkurs.** Wenn wir Zahlen schreiben, verwenden wir normalerweise die üblichen zehn Ziffern. Der Trick, mit dem man auf einheitliche und elegante Weise mit diesen zehn Ziffern auch Zahlen schreiben kann, die viel größer sind als *neun*, stammt aus Indien: Eine Ziffer repräsentiert eine unterschiedliche Anzahl, je nachdem, wo sie in der Zahl steht. Die Ziffer ganz rechts repräsentiert Einer, die Ziffer weiter links davon Zehner, die nächste Ziffer Hunderter und so weiter. Allgemeiner gilt für eine  $n$ -stellige Zahl  $a$  mit Ziffern  $a_0, \dots, a_n \in \{0, 1, 2, \dots, 9\}$ , wobei  $a_0$  die Ziffer ganz rechts sei:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0.$$

Aber warum gerade zehn Ziffern? Nun, das hat keinen besonderen Grund abgesehen davon, dass dies eine Zahl ist, die gewissermaßen auf der Hand liegt: Der Mensch hat nunmal zehn Finger und zehn Zehen (nicht umsonst bedeutet das englische Wort “digit” sowohl Finger als auch Ziffer). Wir können genauso gut ein Zahlensystem entwickeln, das mit nur zwei Ziffern auskommt, sagen wir den Ziffern 0 und 1. Die Zahlen null bis zwölf in diesem System sind:

0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, 1100




Für die Zahlen null und eins konnten wir direkt die Ziffern verwenden. Für die Zahl zwei benötigen wir bereits die „Zweierstelle“ und ab der Zahl vier die „Viererstelle“. Dieses System, das nur mit 0 und 1 auskommt, wird *Binärsystem* genannt. Im Gegensatz dazu heißt das übliche System mit 10 Ziffern *Dezimalsystem*. In diesem System gilt für eine  $n$ -stellige Zahl  $a$  mit Ziffern  $a_0, \dots, a_n \in \{0, 1\}$ :

$$a = a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} \dots + a_1 \cdot 2 + a_0.$$

**Aufgabe.** Rechne um!

- Vom Dezimal- ins Binärsystem: a) 13 b)  $-5$  c) 21 d) 64
- Vom Binär- ins Dezimalsystem: a) 11111 b) 1101 c)  $-11010$  d) 10101010

Nun wollen wir das Spiel mit Hilfe von Binärzahlen analysieren: Angenommen, du bist dran und auf dem Tisch liegen drei Haufen von Steinen. Wir schreiben neben jeden Haufen die Anzahl von Steinen als Zahl im Binärsystem:

Anzahl	Haufen
110	
11	
1010	

Achte darauf, dass dabei alle Binärzahlen rechts ausgerichtet sind und die Einerstelle, die Zweierstelle, die Viererstelle usw. der Binärzahlen in einer Spalte untereinander stehen. Nun betrachten wir jede Spalte für sich genommen und zählen in dieser Spalte die Anzahl der Einsen. Was für uns wichtig ist, ist ob diese Anzahl gerade oder ungerade ist. Oben haben wir vier Spalten (da die größte Zahl von Steinen in einem Haufen, die Zehn, vier Binärziffern lang ist): in der ersten steht nur eine Eins, ebenso in der zweiten und vierten Spalte. In der dritten Spalte stehen drei Einsen. Also steht in jeder Spalte eine ungerade Anzahl von Einsen. Unser Ziel ist es, zu erreichen, dass in jeder Spalte eine gerade Anzahl an Einsen steht. Warum wir das wollen wird gleich klarwerden. Wie können wir dieses Ziel erreichen? Wir könnten im obigen Beispiel die 1010 durch eine 101 ersetzen. Da 101 im Binärsystem für die Fünf steht, müssten wir somit vom Haufen mit zehn Steinen fünf Steine wegnehmen, sodass fünf Steine übrig bleiben.

Gibt es immer solch einen Zug, der dafür sorgt, dass in jeder Spalte eine gerade Anzahl von Einsen steht? Ja, immer dann, wenn dies vor unserem Zug nicht der Fall ist. Ermittle dazu die erste Spalte von links, in der eine ungerade Anzahl an Einsen steht, und wähle einen Haufen aus, dessen Zeile in dieser Spalte eine Eins stehen hat (warum gibt es einen solchen

immer?). Im Beispiel oben ist das der letzte Haufen mit zehn Steinen, da dies die einzige Zeile in der Tabelle ist, in der die Binärzahl vier Ziffern lang ist. Wir können die Ziffern dieser Binärzahl so verändern, sodass danach in jeder Spalte eine gerade Anzahl an Einsen steht. Dabei wird die Zahl auch immer kleiner, denn die erste Ziffer (von links) die wir verändern, ist eine Eins. Sie wird zu einer Null. Egal, wie sich die Ziffern rechts davon ändern, die Zahl wird dadurch kleiner als die ursprüngliche Zahl. Eine ähnliche Situation ist die folgende: Wenn sich zwei Dezimalzahlen nur in der Einerstelle, Zehnerstelle und Hunderterstelle voneinander unterscheiden, aber die erste Zahl auf der Hunderterterstelle eine Vier und die zweite Zahl dort eine Drei stehen hat, dann ist die erste Zahl auf jeden Fall größer als die zweite. Um dies zu entscheiden mussten wir uns gar nicht erst die Zehner- und die Einerstelle ansehen.

Bleibt noch zu erklären, warum wir überhaupt erreichen wollen, dass die Anzahl von Einsen nach unserem Zug in jeder Spalte gerade ist. Dazu überlegen wir, was nach dem Zug unseres Gegners der Fall sein wird: Der Gegner muss von genau einem Haufen Steine entfernen. Dadurch ändert er in der Binärdarstellung der Anzahl der Steine dieses Haufens mindestens eine Ziffer. Dadurch wird die Anzahl der Einsen in mindestens einer Spalte wieder ungerade. Dann können wir mit unserem Zug wieder erreichen, dass die Anzahl an Einsen in jeder Spalte gerade ist. Der darauffolgende Zug des Gegners wird wieder dafür sorgen, dass die Anzahl an Einsen in mindestens einer Spalte ungerade ist, usw. Also ist jedes Mal, wenn wir an der Reihe sind, die Anzahl an Einsen in mindestens einer Spalte ungerade. Aber dann können nicht alle Haufen leer sein! Das heißt, wir können mit dieser Strategie nicht verlieren. Also gewinnen wir damit.

Wenn beide Spieler diese Strategie kennen, dann hängt der Ausgang des Spiels nur von der Anfangssituation ab: Wenn zu Beginn die Anzahl von Einsen in jeder Spalte gerade ist, dann verliert der Spieler, der anfängt, sonst gewinnt er.

**Aufgabe.** Wer gewinnt in den folgenden Spielsituationen, wenn du und dein Gegner die Gewinnstrategie kennen und du an der Reihe bist?

Anzahl	Haufen	Anzahl	Haufen	Anzahl	Haufen
1	●	1001	●●●●●●●●	1001	●●●●●●●●
10	●●	11	●●●	1001	●●●●●●●●
11	●●●	1	●	111	●●●●●●●
100	●●●●	1011	●●●●●●●●	111	●●●●●●●
101	●●●●●				

Zusatzfrage: Gibt es in der letzten Spielsituation auch noch eine einfachere Spielstrategie für deinen Gegenspieler?

**Aufgabe.** Spiele dieses Spiel gegen deine Freunde/Eltern/Geschwister. Erkläre ihnen nach einigen Runden die Gewinnstrategie.

7. und 21. Februar 2014

## 4 Vollständige Induktion

Übungszettel vom 7. Februar 2014: <http://timbaumann.info/mathezirkel-kurs/uebung5.pdf>

Vollständige Induktion ist eines der grundlegenden mathematischen Beweisverfahren. Vollständige Induktion benutzt man immer dafür, um zu zeigen, dass eine bestimmte Aussage für alle natürlichen Zahlen gilt. Zum Beispiel:

**Aufgabe.** Zeige, dass für alle natürlichen Zahlen  $n \in \mathbb{N}$  die folgende Formel gilt:

$$\frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \dots + \frac{1}{2^{n-1}} + \frac{1}{2^n} = 1 - \frac{1}{2^n}.$$

Wir können nun hergehen und diese Formel für spezielle Werte von  $n$  nachrechnen, z. B. für  $n = 1$  oder  $n = 5$  oder (mithilfe eines Computers) für alle natürlichen Zahlen  $n$  kleiner als eine Million.

Wir können uns auch intuitiv klar machen, warum diese Formel gilt: Wir stellen uns einen Zahlenstrahl vor. Wir beginnen bei der Zahl  $\frac{1}{2}$ . Dann addieren wir  $\frac{1}{4}$ , also die Hälfte des Abstands von  $\frac{1}{2}$  zu 1. Wir befinden uns dann bei  $\frac{3}{4}$ . Dann addieren wir  $\frac{1}{8}$ , also die Hälfte des Abstandes von  $\frac{3}{4}$  zu 1. Wenn wir so weitermachen, halbiert sich der Abstand von unserer aktuellen Zahl zur Zahl 1 in jedem Schritt. Und das ist ziemlich genau die Aussage der Aufgabe.

Nun ist aber das Nachrechnen der Formel für konkrete natürliche Zahlen kein Beweis der Aufgabe. Wir können schließlich nicht die Formel für alle natürlichen Zahlen durch einzelnes Nachrechnen prüfen, denn es gibt ja unendlich viele natürliche Zahlen. Die zweite Überlegung ist schon deutlich näher an einem mathematischen Beweis (der nachfolgende Beweis folgt in gewisser Weise sogar den gleichen Überlegungen). Wir wollen nun die Aufgabe mathematisch ganz korrekt durch vollständige Induktion beweisen. Um uns das Leben einfacher zu machen, führen wir davor aber noch etwas Notation ein:

**Notation.** In obiger Aufgabe summieren wir

$$\frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \dots + \frac{1}{2^{n-1}} + \frac{1}{2^n} = 1 - \frac{1}{2^n},$$

also alle Brüche  $\frac{1}{2^k}$ , wobei  $k$  nacheinander die Werte 1 bis  $n$  annimmt. Für solche Summen verwendet man folgende abkürzende Schreibweise:

$$\sum_{k=1}^n \frac{1}{2^k} = \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \dots + \frac{1}{2^{n-1}} + \frac{1}{2^n} = 1 - \frac{1}{2^n}.$$

Der griechische Buchstabe  $\Sigma$  heißt Sigma, die Zeilen  $k = 1$  darunter und  $n$  darüber bedeuten, dass zuerst  $k = 1$ , dann  $k = 2$ , usw. bis  $k = n$  gilt. Die Variable  $k$  wird auch Zählvariable genannt. Die Werte des Ausdrucks  $\frac{1}{2^k}$  rechts neben  $\Sigma$  werden für all diese Werte von  $k$  aufaddiert.

Mit dieser Notation wird die Formel einfacher und damit überschaubarer. Außerdem spart man sich viele Auslassungspunkte.

Weitere Beispiele für die Verwendung dieser Summennotation sind:

$$\begin{aligned} \sum_{k=1}^5 k &= 1 + 2 + 3 + 4 + 5 = 15 \\ \sum_{k=0}^n 2^k &= 2^0 + 2^1 + 2^2 + \dots + 2^n \\ \sum_{j=1}^k \frac{1}{j} &= \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{k} \end{aligned}$$

Das letzte Beispiel zeigt, dass wir für die Zählvariable auch andere Buchstaben außer  $k$  benutzen können, und statt bis  $n$  auch bis  $k$  summieren können.

Wir können damit die obige Aufgabe folgendermaßen umschreiben:

**Aufgabe.** Zeige, dass für alle natürlichen Zahlen  $n \in \mathbb{N}$  die folgende Formel gilt:

$$\sum_{k=1}^n \frac{1}{2^k} = 1 - \frac{1}{2^n}.$$

*Beweis.* Wir führen Induktion über  $n$  durch:

*Induktionsanfang:* Die Formel stimmt für  $n = 1$ , wie wir leicht nachrechnen:

$$\sum_{k=1}^1 \frac{1}{2^k} = \sum_{k=1}^1 \frac{1}{2^k} = \frac{1}{2^1} = 1 - \frac{1}{2^1} = 1 - \frac{1}{2^n}$$

*Induktionsschritt:* Wir nehmen an, dass die Formel für eine bestimmte natürliche Zahl  $n \in \mathbb{N}$  gilt und zeigen, dass die Formel dann auch für die nächstgrößere natürliche Zahl, also  $n+1$ , gilt. Dazu rechnen wir:

$$\sum_{k=1}^{n+1} \frac{1}{2^k} = \left( \sum_{k=1}^n \frac{1}{2^k} \right) + \frac{1}{2^{n+1}} = \left( 1 - \frac{1}{2^n} \right) + \frac{1}{2^{n+1}} = 1 - \frac{2}{2^{n+1}} + \frac{1}{2^{n+1}} = 1 - \frac{1}{2^{n+1}}$$

Bei der ersten Gleichheit steht dabei auf beiden Seiten genau dasselbe, nur jeweils mit etwas anderer Notation. Links wurde die Summennotation für das Addieren von  $n+1$  Zahlen verwendet, rechts nur für  $n$  Zahlen. Dafür wurde rechts der letzte Summand extra hinzuaddiert. Die zweite Gleichheit folgt aus der Annahme (s. o.), dass die Formel aus der Aufgabe für die Zahl  $n$  stimmt. Wir konnten also die Formel direkt für den eingeklammerten Ausdruck anwenden. Die restlichen Gleichheiten sind Routine-Rechnungen.  $\square$

Warum nun ist dies ein korrekter Beweis für die Aufgabe? Nun, wir können dem Beweis direkt entnehmen, dass die Formel für die kleinste natürliche Zahl, also  $n = 1$  gilt. Das haben wir im Teil „Induktionsanfang“ direkt nachgerechnet. Dann gilt aber auch die Formel für  $n = 2$ , denn: Die Formel gilt für  $n = 1$  und das Argument im Teil „Induktionsschritt“ sagt uns, dass deswegen auch die Formel für  $1 + 1 = 2$  gilt. Dann gilt aber auch die Formel für  $n = 3$ , denn: Die Formel gilt für  $n = 2$  und das Argument im Teil „Induktionsschritt“ sagt uns, dass deswegen auch die Formel für  $2 + 1 = 3$  gilt. Dann gilt aber auch die Formel für  $n = 4$ , denn: Die Formel gilt für  $n = 3$  und das Argument im Teil „Induktionsschritt“ sagt uns, dass deswegen auch die Formel für  $3 + 1 = 4$  gilt. Und so weiter und so fort. Da wir so jede natürliche Zahl erreichen können, gilt die Formel für alle natürlichen Zahlen.

Wir wollen nochmal allgemein zusammenfassen, wie ein Beweis durch vollständige Induktion aufgebaut ist. Wenn wir eine mathematische Aussage für alle natürlichen Zahlen  $n \in \mathbb{N}$  beweisen wollen, dann reicht es aus, zu zeigen:

- Die Aussage gilt für die kleinste natürliche Zahl  $n$ , also  $n = 1$  (*Induktionsanfang*)



- Wenn die Aussage für eine natürliche Zahl  $n$  gilt, dann gilt sie auch für die nächstgrößere natürliche Zahl  $n + 1$  (*Induktionsschritt*).

Im Induktionsschritt dürfen wir also voraussetzen, dass die Aussage, die wir zeigen wollen, für die Zahl  $n$  gilt. Diese Voraussetzung nennt man auch *Induktionsannahme* oder *Induktionshypothese*. Unsere Aufgabe ist es, zu zeigen, dass die Aussage dann auch für  $n + 1$  gilt.

**Exkurs.** Vollständige Induktion wird oft schlicht auch nur Induktion genannt. Das Adjektiv „vollständig“ dient zur Abgrenzung der mathematischen Induktion von der philosophischen Induktion, einem Prinzip des Schlussfolgerns, dass die Ableitung von abstrakten Gesetzmäßigkeiten von konkreten Beobachtungen beschreibt.

Am besten versteht man Induktion und wann man sie wirkungsvoll einsetzt, indem man Aufgaben rechnet. Darum:

**Aufgabe.** Zeige: Für alle natürlichen Zahlen  $n \in \mathbb{N}$  gilt:

$$\sum_{k=1}^n k = \frac{n \cdot (n + 1)}{2}.$$

Zu dieser Aufgabe gibt es eine Geschichte, die in vielen Mathematik-Büchern zu finden ist: Der später berühmte Mathematiker Carl Friedrich Gauß bekam als Schüler von seinem Lehrer die Aufgabe, alle Zahlen von 1 bis 100 zu addieren. Der Lehrer hatte damit gerechnet, dass seine Klasse mit dieser Aufgabe einige Zeit beschäftigt sein würde. Umso verblüffter war er, als der kleine Gauß schon nach kurzer Zeit die Lösung hatte:  $\sum_{i=1}^{100} i = 5050$ . Wie hatte Gauß diese Aufgabe so schnell gelöst? Seine Idee war, die Zahlen von 1 bis 101 in folgende Paare aufzuteilen:

$$\begin{array}{cccccc} 1 & 2 & 3 & \cdots & 49 & 50 \\ + & + & + & \cdots & + & + \\ 100 & 99 & 98 & \cdots & 52 & 51 \\ = & = & = & \cdots & = & = \\ 101 & 101 & 101 & \cdots & 101 & 101 \end{array}$$

Die Summe jedes Paares ist dabei 101. Wie man leicht sieht, gibt es genau 50 solcher Paare. Also ist die Summe aller Zahlen von 1 bis 100 gleich  $50 \cdot 101 = 5050$ .

Wir können auch in die Formel aus der Aufgabe  $n = 100$  setzen und kommen so auf dieselbe Lösung. Der Term  $\frac{n \cdot (n+1)}{2}$  lässt sich (für gerade Zahlen  $n$ ) folgendermaßen interpretieren: Es gibt  $\frac{n}{2}$  Paare von Zahlen, deren Summe jeweils  $n + 1$  ist.

Die Begründung der Formel mittels Zahlenpaare wie oben funktioniert für gerade Zahlen. Man kann sich auch überlegen, dass die Formel auch für ungerade Zahlen gilt. Diese Überlegungen bilden zusammen schon einen Beweis der Formel. Einen alternativen Beweis kann man per Induktion führen:

*Beweis. Induktionsanfang:* Die Formel stimmt für  $n = 1$ , denn

$$\sum_{k=1}^n k = \sum_{k=1}^1 k = 1 = \frac{1 \cdot 2}{2} = \frac{n \cdot (n + 1)}{2}.$$

*Induktionsschritt:* Angenommen, die Formel gilt für die natürliche Zahl  $n$ , also  $\sum_{k=1}^n k = \frac{n \cdot (n+1)}{2}$ . Wir müssen zeigen, dass die Formel dann auch für  $n+1$  stimmt, also dass gilt:

$$\sum_{k=1}^{n+1} k = \frac{(n+1) \cdot ((n+1) + 1)}{2} \quad \left( = \frac{(n+1) \cdot (n+2)}{2} \right).$$

Dies können wir mithilfe der Induktionshypothese leicht nachrechnen:

$$\begin{aligned} \sum_{k=1}^{n+1} k &= \sum_{k=1}^n k + (n+1) \stackrel{\text{IH}}{=} \frac{n \cdot (n+1)}{2} + (n+1) = \frac{n \cdot (n+1)}{2} + \frac{2 \cdot (n+1)}{2} = \\ &= \frac{n \cdot (n+1) + 2 \cdot (n+1)}{2} = \frac{(n+2) \cdot (n+1)}{2} = \frac{(n+1) \cdot (n+2)}{2}. \end{aligned}$$

Bei der ersten Gleichheit steht auf beiden Seiten wieder genau dasselbe, nur mit anderer Notation. Bei der mit IH beschrifteten Gleichheit haben wir die Induktionshypothese (abgekürzt IH) gebraucht. Hinter der vorletzten Gleichheit steckt das Distributiv-, hinter der letzten Gleichheit das Kommutativgesetz.  $\square$

Bislang haben wir mit Induktion nur Aufgaben gelöst, in denen man eine Gleichheit zeigen sollte. Man Induktion aber auch für Ungleichungen anwenden:

**Aufgabe.** Zeige: Für alle natürlichen Zahlen  $n \geq 4$  gilt:

$$n! \geq 2^n \geq n^2.$$

**Erinnerung.** Der Ausdruck  $n!$  (für eine natürliche Zahl  $n$ ) wird „ $n$  Fakultät“ ausgesprochen und ist definiert als das Produkt aller Zahlen von 1 bis  $n$ , also

$$n! := 1 \cdot 2 \cdot \dots \cdot n.$$

Man setzt üblicherweise  $0! := 1$ . Es gilt dann offensichtlich für alle  $n \geq 1$ :  $n! = n \cdot (n-1)!$

Die Fakultät wird häufig für die Beantwortung von Aufgaben wie „Wie viele Möglichkeiten gibt es,  $n$  Personen auf  $n$  Sitzplätze zu verteilen“ gebraucht (Antwort:  $n!$ ).

Außerdem: Der Doppelpunkt vor dem Gleichheitszeichen weist darauf hin, dass die Gleichheit nicht aufgrund einer Rechnung, sondern nach Definition gilt. Wir legen also den Ausdruck links des  $:=$ -Zeichens durch den Ausdruck rechts davon fest.

Abgesehen davon, dass wir es in dieser Aufgabe nicht mit einer Gleichheit zu tun haben, in der auf der linken Seite eine Summe vorkommt, hat diese Aufgabe noch einen anderen Unterschied zu den bisher gerechneten Aufgaben: Bis jetzt sollten wir zeigen, dass eine Formel für alle natürlichen Zahlen gilt. In dieser Aufgabe sollen wir die Ungleichung nicht für alle natürlichen Zahlen, sondern nur für alle natürlichen Zahlen, die größer oder gleich 4 sind, zeigen. Für die Zahlen 1, 2 und 3 ist die Behauptung nämlich schlicht falsch:

$n$	$n!$	$2^n$	$n^2$
0	1	1	0
1	1	2	1
2	2	4	4
3	6	8	9
4	24	16	16
5	120	32	25

In der Aufgaben müssen wir genau genommen zwei Ungleichungen zeigen: Die erste Ungleichung  $n! \geq 2^n$  und die zweite Ungleichung  $2^n \geq n^2$  für je  $n \geq 4$ . Wir können beide Ungleichungen jeweils einzeln wie die vorherigen Aufgaben mit Induktion beweisen, mit dem Unterschied, dass wir die Induktion bei der Zahl 4 starten:

*Beweis.* • Erste Ungleichung ( $n! \geq 2^n$ ):

*Induktionsanfang* ( $n = 4$ ): Durch Rechnung:

$$n! = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24 \geq 16 = 2^4 = 2^n.$$

*Induktionsschritt* ( $n \rightarrow n+1$ , wobei  $n \geq 4$ ): Wir rechnen:

$$(n+1)! = (n+1) \cdot n! \stackrel{\text{IH}}{\geq} (n+1) \cdot 2^n \geq 2 \cdot 2^n = 2^{n+1}.$$

In dieser Rechnung haben wir folgende Tatsache zweimal gebraucht: Für drei positive natürliche (oder auch rationale oder reelle Zahlen)  $a, b, c$  gilt: Wenn  $a \geq b$  ist, dann ist auch  $a \cdot c \geq b \cdot c$ . Hinter dieser der ersten Ungleichung steckt die Induktionshypothese, dass  $n! \geq 2^n$ , zusammen mit dieser Tatsache ( $a = n!$ ,  $b = 2^n$ ,  $c = n+1$ ). Die zweite Annahme folgt mit  $n+1 \geq n \geq 4 \geq 2$  und der Tatsache angewendet auf  $a = n+1$ ,  $b = 2$  und  $c = n+1$ .

- Um die zweite Ungleichung zu beweisen, brauchen wir noch eine weitere Ungleichung, die wir per Induktion beweisen, nämlich: Für alle  $n \geq 3$  gilt  $2^n \geq 2n+1$  (Hilfsbehauptung).

*Induktionsanfang* ( $n = 3$ ): Durch Rechnung:

$$2^n = 2^3 = 8 \geq 7 = 2 \cdot 3 + 1 = 2 \cdot n + 1.$$

*Induktionsschritt* ( $n \rightarrow n+1$ , wobei  $n \geq 3$ ):

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \stackrel{\text{IH}}{\geq} 2 \cdot (2n+1) = 4n+2 \geq 2n+2+n = 2 \cdot (n+1) + n \geq \\ &\geq 2 \cdot (n+1) + 3 \geq 2 \cdot (n+1) + 1. \end{aligned}$$

- Zweite Ungleichung ( $2^n \geq n^2$ ):

*Induktionsanfang* ( $n = 4$ ): Durch Rechnung:

$$2^n = 2^4 = 16 = 4^2 = n^2.$$

Da also  $2^n = n^2$ , gilt auch  $2^n \geq n^2$  (= ist ein Spezialfall von  $\geq$ ).

*Induktionsschritt* ( $n \rightarrow n+1$ , wobei  $n \geq 4$ ): Hier ist es einfacher, von hinten nach vorne zu rechnen, also  $(n+1)^2 \leq 2^{n+1}$  zu zeigen:

$$(n+1)^2 = n^2 + 2n + 1 \stackrel{\text{IH}}{\leq} 2^n + 2n + 1 \leq 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}.$$

Die Gültigkeit des ersten  $\leq$ -Zeichens folgt aus unserer Induktionshypothese ( $2^n \geq n^2$ ), die des zweiten  $\leq$ -Zeichens durch unsere Hilfsbehauptung, die wir gerade eben in Punkt zwei bewiesen haben.  $\square$

Folgende Aufgabe stammt (leicht abgewandelt) aus der 51. Mathematik-Olympiade. Obwohl sie eine Aufgabe für die 11. bis 13. Klasse ist, lässt sie sich sehr einfach durch Induktion lösen:

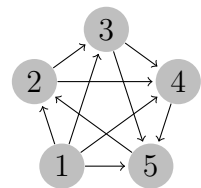
**Aufgabe** (Turnier). In einem Fechtturnier mit  $2^n$  Teilnehmern kämpft jeder Fechter genau einmal gegen jeden anderen. Kein Kampf endet unentschieden. Eine Reporterin möchte nacheinander Einzelinterviews mit  $n+1$  Fechtern führen. Diese sollen so ausgewählt werden, dass jeder interviewte Fechter gegen alle Fechter, die vor ihm interviewt wurden, gesiegt hat.

Zeige, dass für alle natürlichen Zahlen  $n$  die Reporterin eine entsprechende Auswahl von Fechtern für die Interviews treffen kann.

*Beweis. Induktionsanfang* ( $n = 1$ ): Dann gibt es  $2^n = 2^1 = 2$  Fechter, die Reporterin will  $n+1 = 1+1 = 2$  Fechter, also alle beide interviewen. Es findet genau ein Fechtkampf statt. Die Reporterin erreicht ihr Ziel, wenn sie zuerst den Verlierer, dann den Gewinner interviewt.

*Induktionsschritt* ( $n \rightarrow n+1$ ): Es kämpfen insgesamt  $2^{n+1}$  Fechter gegeneinander, also jeder Fechter gegen die anderen  $2^{n+1} - 1$  Fechter. Durchschnittlich gewinnt jeder Fechter die Hälfte seiner Duelle, also  $\frac{2^{n+1}-1}{2} = \frac{2^{n+1}}{2} - \frac{1}{2} = 2^n - \frac{1}{2}$  viele. Da dieser Durchschnitt keine ganze Zahl ist, muss es mindestens einen Fechter geben, der mindestens  $2^n$  (die nächstgrößere ganze Zahl über  $2^n - \frac{1}{2}$ ) Duelle gewonnen hat. Unter den  $2^n$  Verlierern dieser Duelle kann die Reporterin nach Induktionsannahme eine gewünschte Reihenfolge von  $n$  Interviewpartnern finden. Wenn sie danach den Sieger dieser Duelle, also den Fechter, der gegen die  $2^n$  zuvor interviewten Fechter gewonnen hat, interviewt, hat sie ihr Ziel erreicht.  $\square$

Auf der rechten Seite siehst du einen gesättigten gerichteten Graphen mit 5 Knoten (graue Kreise). Die Pfeile zwischen den Knoten werden auch *Kanten* genannt. Wir sagen, dass wir einen Knoten  $B$  von einem anderen Knoten  $A$  direkt erreichen können, wenn eine Kante von  $A$  nach  $B$  verläuft (also die Pfeilspitze zu  $B$  zeigt). Ein Knoten  $B$  kann von einem anderen Knoten  $A$  in zwei Schritten erreicht werden, wenn es einen Knoten  $C$  gibt, sodass  $C$  von  $A$  direkt erreichbar ist und  $B$  von  $C$  direkt erreichbar ist.



Im Beispiel ist der Knoten 3 vom Knoten 1 in zwei Schritten erreichbar, aber andersrum der Knoten 1 nicht vom Knoten 3 in zwei Schritten erreichbar. Außerdem ist der Knoten 2 von jedem anderen Knoten in höchstens zwei Schritten erreichbar.

**Aufgabe.** Zeige, dass es in jedem gesättigten gerichteten Graphen mit  $n$  Knoten einen Knoten gibt, der von jedem anderen Knoten in höchstens zwei Schritten erreicht werden kann.

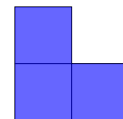
*Beweis. Induktionsanfang* ( $n = 1$ ): Wir haben also nur einen Knoten im Graph. Dieser kann offensichtlich von jedem anderen Knoten erreicht werden, denn es gibt ja gar keinen anderen Knoten.

*Induktionsschritt* ( $n \rightarrow n+1$ ): Wir greifen uns aus einem gesättigten Graphen mit  $n+1$  Knoten einen Knoten  $K$  wahllos heraus. Die restlichen  $n$  Knoten und deren Knoten untereinander bilden einen gerichteten Graphen mit  $n$  Knoten. Nach Induktionsannahme gibt es unter ihnen einen Knoten, der von den restlichen  $n-1$  Knoten in höchstens zwei Schritten erreicht werden kann. Wir nennen diesen Knoten  $A$ . Die Knoten, die direkt mit  $A$  verbunden sind, nennen wir D-Knoten („D“ für direkt). Nun fügen wir den am Anfang herausgenommenen Knoten  $K$  und all seine Kanten wieder hinzu. Es tritt nun einer der folgenden zwei Fälle ein:

- Alle D-Knoten und auch  $A$  sind direkt mit  $K$  verbunden. Dann ist  $K$  ein Knoten, wie er in der Aufgabenstellung gesucht wird.
- Entweder ist  $K$  direkt mit  $A$  verbunden, oder es gibt einen D-Knoten, zu dem  $K$  direkt verbunden ist (also existiert eine Kante von  $K$  zu einem D-Knoten). In beiden Fällen ist der Knoten  $A$  von  $K$  in höchstens zwei Schritten erreichbar. Da  $A$  auch von jedem anderen Knoten in höchstens 2 Schritten erreichbar ist, ist  $A$  der gesuchte Knoten.  $\square$

**Achtung.** Nicht alle Induktionsbeweise, die du in Büchern findest, folgen in allen Details dem hier vorgestellten Schema. Insbesondere wird im Induktionsschritt oft gezeigt, dass eine Aussage für die Zahl  $n$  ( $n \geq 2$ ) gilt, wenn die Aussage für die Zahl  $n-1$  gilt. Man schließt im Induktionsschritt also nicht von  $n$  auf  $n+1$ , sondern von  $n-1$  auf  $n$ . Für die Gültigkeit der Induktion spielt das aber keine Rolle. Als Beispiel ist die nächste Aufgabe mit dieser Konvention bearbeitet.

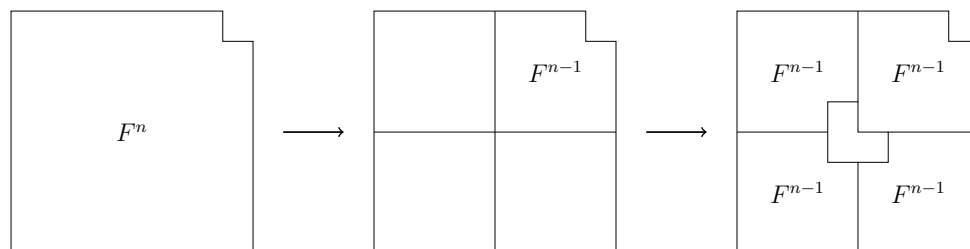
Ein Tromino ist ein Stein, der zwei Schachbrettfelder breit und zwei Schachbrettfelder hoch ist und genau drei Schachbrettfelder überdeckt, also gewissermaßen ein  $(2 \times 2)$ -Quadrat, aus dem eine Ecke entfernt wurde (siehe rechts).



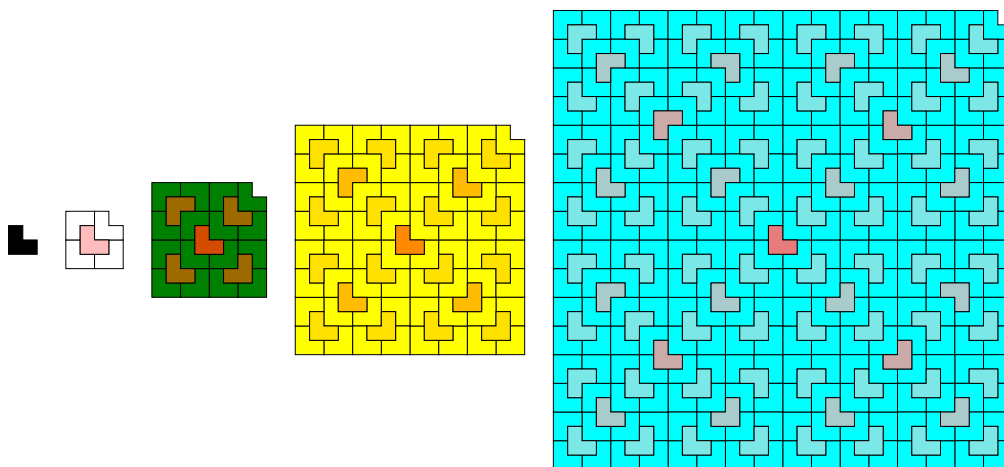
**Aufgabe.** Zeige per Induktion, dass es für alle  $n \in \mathbb{N}$  möglich ist, ein quadratisches Brett, das  $2^n$  Felder breit und hoch ist, und aus dem eine Ecke entfernt wurde, mit Trominos zu belegen.

*Beweis. Induktionsanfang* ( $n = 1$ ): Dann ist das Brett je  $2^n = 2^1 = 2$  Felder lang und breit, wobei eine Ecke herausgeschnitten ist. Kurz: Das Feld hat die Form eines Trominos.

*Induktionsschritt* ( $n-1 \rightarrow n$ , wobei  $n \geq 2$ ): Wir beschriften ein  $(2^k \times 2^k)$ -Brett, aus dem eine Ecke entfernt wurde, mit  $F^k$ . Nach Induktionsvoraussetzung ist also das Brett  $F^{n-1}$  mit Trominos belegbar und wir müssen zeigen, dass auch das Brett  $F^n$  mit Trominos belegt werden kann. Dazu teilen wir das Brett  $F^n$  in vier quadratische Stücke mit Seitenlänge  $2^{n-1}$ . Dabei entsteht ein  $F^{n-1}$ -Brett und drei vollständige  $(n-1 \times n-1)$ -Bretter (mit allen Ecken). Wir legen ein Tetromino in die Mitte des  $F^n$ -Bretts, sodass es je eine Ecke der drei vollständigen  $(n-1 \times n-1)$ -Bretter bedeckt. Damit bleiben uns noch vier  $F^{n-1}$ -Bretter übrig, die wir nach Induktionsannahme belegen können.  $\square$



Mit diesem Beweis als Anleitung können wir leicht  $F^n$ -Bretter für beliebiges  $n$  selbst mit Trominos belegen. Oder wir können ein Computerprogramm schreiben, das uns die Belegung als Graphik ausgibt (hier  $n = 1, \dots, 4$ ):



**Exkurs.** Das Computerprogramm, das obiges Bild erzeugt hat, ist mit Rekursion geschrieben. Rekursion bedeutet, dass eine Funktion im Programm sich selbst aufruft, um ein Teilproblem zu lösen. In diesem Programm verwendet die Zeichenfunktion sich selbst um die vier  $F^{n-1}$ -Teilbretter zu füllen. Es ist dabei kein Zufall, dass wir zum Visualisieren eines induktiven Beweises Rekursion verwendet haben, denn: Rekursion ist sehr eng verwandt mit Induktion.

14. März 2014

## 5 Gerechte Wahlen

Wir führen eine Wahl zwischen drei Kandidaten  $A$ ,  $B$  und  $C$  durch. Dazu könnten wir jedem Wähler einen Zettel austeilen, auf dem er seinen favorisierten Kandidaten ankreuzt. Der Kandidat mit den meisten Stimmen soll gewinnen. Dieses Wahlverfahren hat aber ein Problem: Angenommen, zwei der Kandidaten, sagen wir  $A$  und  $B$  haben inhaltlich ähnliche politische Positionen. Dann kann es sein, dass diese beiden Kandidaten sich gegenseitig Stimmen wegnehmen und dadurch Kandidat  $C$  am meisten Stimmen von allen Kandidaten erhält, obwohl seine Politik von weniger Wählern unterstützt wird als die Politik der Kandidaten  $A$  und  $B$  zusammen. Das wäre ein schlechtes Wahlergebnis. Wir wollen deshalb den Wählern die Möglichkeit geben, nicht nur ihren favorisierten Kandidaten anzukreuzen, sondern die Kandidaten nach Präferenz zu sortieren. Wenn jemand z. B.  $A > C > B$  auf seinen Wahlzettel schreibt, dann bedeutet das, dass der Kandidat  $A$  seine erste Wahl, Kandidat  $C$  seine zweite Wahl und Kandidat  $B$  seine dritte Wahl ist. Wähler von  $A$  würden in obiger Situation vermutlich  $A > B > C$  auf ihren Zettel schreiben und Wähler von  $B$  schreiben wahrscheinlich  $B > A > C$  auf ihre Zettel. Dadurch ist zu hoffen, dass einer der Kandidaten  $A$  und  $B$  auch im Gesamtergebnis vorne liegen wird.

Bei unserer Abstimmung erhalten wir folgendes Wahlergebnis:

Reihenfolge	Stimmen
$A > B > C$	6
$A > C > B$	0
$B > A > C$	5
$B > C > A$	2
$C > A > B$	5
$C > B > A$	3

Wer hat diese Wahl gewonnen? Dafür können wir uns mehrere Auswertungsverfahren überlegen:

1. Der Kandidat gewinnt, der am häufigsten als erste Wahl gelistet wurde.
2. Wir können Stichwahlen zwischen je zwei Kandidaten simulieren, da wir ja für je zwei Kandidaten und für jeden Wähler wissen, welchen Kandidaten er bei einer Stichwahl vorziehen würde. Gibt es einen Kandidaten, der gegen alle anderen Kandidaten gewinnt? Wenn ja, dann soll er der Wahlsieger sein.
3. Wir vergeben Punkte: Für jeden ersten Platz gibt es drei Punkte, für jeden zweiten Platz zwei Punkte und für jeden dritten Platz einen Punkt. Die Wahl gewinnt, wer die meisten Punkte hat.

In diesem Fall sind die Gesamtergebnisse:

1. Kandidat  $C$  hat 8 Erststimmen, Kandidat  $B$  hat 7 Erststimmen und Kandidat  $A$  hat 6 Erststimmen. Also gewinnt Kandidat  $C$  und die Gesamtreihenfolge ist  $C > B > A$ .
2. Bei einer Stichwahl zwischen  $A$  und  $B$  stimmen 11 Wähler für  $A$  und 10 Wähler für  $B$ . Wenn  $A$  und  $C$  in einer Stichwahl gegeneinander antreten, so erhält  $a$  wieder 11 stimmen und  $C$  erhält 10 stimmen. In einer Stichwahl zwischen  $B$  und  $C$  bekommt  $b$  13 und  $c$  8 Stimmen. Somit gewinnt Kandidat  $A$  und die Gesamtreihenfolge ist  $A > B > C$ .
3. Der Punktestand ist: Kandidat  $A$  hat 43 Punkte, Kandidat  $B$  44 Punkte und Kandidat  $C$  39 Punkte. Es gewinnt  $B$  und die Gesamtreihenfolge ist  $B > A > C$ .

Es fällt auf, dass bei den drei Auswertungsverfahren jeweils ein anderer Kandidat den Gesamtsieg davonträgt. Das Verfahren 1 sollten wir ausschließen, da es genau der Mehrheitswahl entspricht, dessen Nachteil wir ja beheben wollten. Die Verfahren 2 und 3 jedoch, erscheinen beide sinnvoll. Es gibt also keinen klaren Sieger bei dieser Wahl.

**Frage.** Gibt es ein Auswertungsverfahren für solche Wahlen, dass aus den einzelnen Wählerstimmen eine Gesamtreihenfolge ermittelt, von der man behaupten kann, dass sie gerecht ist?

Von solch einem Verfahren würden wir uns ein paar Eigenschaften erwarten:

- (I) Wenn jeder Wähler den Kandidaten  $X$  dem Kandidaten  $Y$  vorzieht, dann sollte auch in der Gesamtreihenfolge  $X$  vor  $Y$  stehen.

- (II) Ob in der Gesamtreihenfolge Kandidat  $X$  vor Kandidat  $Y$  steht, sollte nur von der Reihenfolge dieser Kandidaten untereinander in den einzelnen Stimmen ab. Wo ein dritter Kandidat  $Z$  steht, sollte keine Auswirkung darauf haben. Anders formuliert: Wenn bei zwei Wahlen alle Wähler bei beiden Wahlen die Kandidaten  $X$  und  $Y$  untereinander gleich ordnen (d.h. jeder Wähler wählt in beiden Wahlen entweder  $X > Y$  oder in beiden Wahlen  $Y > X$ ), dann ist auch die Reihenfolge von  $X$  und  $Y$  untereinander in beiden Gesamtergebnissen gleich.
- (III) Es soll keinen „Diktator“ geben, d. h. einen Wähler, der durch seine Stimme alleine das Wahlergebnis festlegt.

*Antwort.* Die vielleicht etwas überraschende Antwort ist: Nein! Jedes Verfahren, das die Eigenschaften (I) und (II) besitzt, verstößt gegen Eigenschaft (III). Es gibt also kein Verfahren, dass alle drei Eigenschaften in sich vereinigt. Dies hat der Nobelpreisträger und Ökonom Kenneth Arrow zuerst bewiesen. Wir führen den Beweis hier in mehreren Schritten:

Angenommen, es gibt  $m \geq 2$  Wähler. Wir stellen uns vor, dass die Wähler in einer festen Reihenfolge aufgestellt und durchnummeriert sind. Zuerst nehmen wir an, dass Kandidat  $B$  auf jedem Stimmzettel den letzten Platz belegt. Dann ist auf jedem Stimmzettel Kandidat  $B$  schlechter als jeder andere Kandidat und muss daher auch in der Gesamtreihenfolge den letzten Platz belegen (wegen Forderung I). Wir betrachten nacheinander die Szenarien 1 bis  $m$ , wobei in dem Szenario  $k$  die Wahl folgendermaßen ausgeht:

Wähler 1	Wähler 2	...	Wähler $k$	Wähler $k+1$	...	Wähler $m$
$B > A > C$	$B > A > C$		$B > A > C$	$A > C > B$		$A > C > B$
oder	oder	...	oder	oder	...	oder
$B > C > A$	$B > C > A$		$B > C > A$	$C > A > B$		$C > A > B$

Kurz zusammengefasst: In Szenario  $k$  stimmen die ersten  $k$  Wähler mit ihrer ersten Stimme für den Kandidaten  $B$ , die restlichen  $m-k$  haben Kandidat  $B$  an Schluss ihrer Liste gesetzt.

Wir haben bereits begründet, dass in Szenario 0 Kandidat  $B$  in der Gesamtreihenfolge an letzter Stelle stehen muss. Mit ähnlicher Begründung gilt: In Szenario  $m$  muss der Kandidat  $B$  an erster Stelle stehen. In einem bestimmten Szenario muss es daher das erste Mal der Fall sein, dass im Gesamtergebnis Kandidat  $B$  vor Kandidat  $A$  steht. Wir bezeichnen mit  $k_{B>A}$  die Nummer dieses Szenarios. Beachte dabei, dass die Positionierung der Kandidaten  $A$  und  $C$  untereinander auf den Wahlzetteln keine Rolle spielt wegen Bedingung (II). Da in Szenario  $k_{B>A} - 1$  noch im Gesamtergebnis noch  $A$  vor  $B$  stand, muss die Stimme des Wählers an Position  $k_{B>A}$  den Ausschlag dazu gegeben haben, dass im Szenario  $k_{B>A}$  der Kandidat  $B$  vor  $A$  im Gesamtergebnis steht. Wir nennen diesen Wähler daher auch den  $B>A$ -Schlüsselwähler.

Wir betrachten nun die folgenden Wahlen:

	Wähler 1	...	Wähler $k_{B>A}-1$	Wähler $k_{B>A}$	Wähler $k_{B>A}+1$	...	Wähler $m$
Wahl 1	$B > C > A$	...	$B > C > A$	$A > B > C$	$A > B > C$	...	$A > B > C$
Wahl 2	$B > C > A$	...	$B > C > A$	$B > A > C$	$A > B > C$	...	$A > B > C$
	oder $C > B > A$		oder $C > B > A$		oder $A > C > B$		oder $A > C > B$

In der ersten Wahl wählen die ersten  $k_{B>A} - 1$  Wähler die Reihenfolge  $B > C > A$  (insbesondere  $B > A$ ), die restlichen Wähler stimmen für die Reihenfolge  $A > B > C$  (insbesondere



$A > B$ ). Da der  $B > A$ -Schlüsselwähler, also der Wähler an Position  $k_{B>A}$ , und die restlichen Wähler  $A > B$  abstimmen, gilt auch im Gesamtergebnis dieser Wahl  $A > B$ . In der ersten Wahl stimmt außerdem jeder Wähler für  $B > C$ . Nach Eigenschaft (I) gilt damit in der Gesamtreihenfolge  $B > C$ . Zusammengefasst wissen wir also das Ergebnis dieser Wahl:  $A > B > C$ .

In der zweiten Wahl stimmen die ersten  $k_{B>A}$  Wähler für  $B > A$ . Somit gilt auch im Gesamtergebnis dieser Wahl  $B > A$ . Außerdem gilt im Gesamtergebnis der zweiten Wahl  $A > C$ , da im Gesamtergebnis der ersten Wahl  $A > C$  gilt und sich die Rangfolge der Kandidaten  $A$  und  $C$  in den einzelnen Stimmabgaben gegenüber der ersten Wahl nicht geändert hat und damit sich deren Reihenfolge im Gesamtergebnis damit auch nicht ändert (Bedingung II). Das Ergebnis der zweiten Wahl ist somit  $B > A > C$ .

Insbesondere gilt in der zweiten Wahl also  $B > C$  im Gesamtergebnis. Da wir aufgrund von Bedingung (II) die Positionierung von Kandidat  $A$  ignorieren dürfen, folgt: Wann immer der  $B>A$ -Schlüsselwähler für  $B > C$  stimmt, dann ist auch im Gesamtergebnis  $B > C$ .

Wir haben bisher die Zahl  $k_{B>A}$  eingeführt und den Wähler an dieser Position den  $B>A$ -Schlüsselwählers genannt. Genauso können wir für zwei Kandidaten  $X, Y \in \{A, B, C\}$  mit  $X \neq Y$  die Zahl  $k_{X>Y}$  und den Begriff des  $X>Y$ -Schlüsselwählers einführen.

Wir haben schon bewiesen: Wenn der  $B>A$ -Schlüsselwähler für  $B > C$  stimmt, dann gilt auch  $B > C$  im Gesamtergebnis. Somit kann der  $B>C$ -Schlüsselwähler nicht an späterer Position kommen als der  $B>A$ -Schlüsselwähler. Der  $C>B$ -Schlüsselwähler dagegen kann nicht an früherer Position kommen als der  $B>A$ -Schlüsselwähler. Denn sonst würde der  $B>A$  Schlüsselwähler für  $B>C$  stimmen, was dazu führen würde, dass auch im Gesamtergebnis  $B>C$  gilt. Es gilt somit:

$$k_{B>C} \leq k_{B>A} \leq k_{C>B}$$

Insbesondere gilt  $k_{B>C} \leq k_{C>B}$ . Da wir nichts spezielles über die Kandidaten  $B$  und  $C$  angenommen haben, folgt aus Symmetriegründen auch die umgekehrte Ungleichung, also  $k_{C>B} \leq k_{B>C}$ . Damit gilt aber  $k_{C>B} = k_{B>C} = k_{B>A}$ .

Aus ähnlichen Überlegungen folgt  $k_{A>B} = k_{A>C} = k_{B>C} = k_{C>B} = k_{A>C} = k_{C>A}$ . Alle Schlüsselwähler sind in Wahrheit also ein- und dieselbe Person! Wir haben schon gesehen, dass wenn diese Person  $B > C$  wählt, dann auch im Gesamtergebnis  $B > C$  gilt. Allgemeiner kann man sich überlegen: Wenn diese Person  $X > Y$  wählt, dann gilt auch im Gesamtergebnis  $X > Y$  für beliebige Kandidaten  $X, Y \in \{A, B, C\}$ . Das Wahlergebnis spiegelt also allein die Wahlentscheidung dieser Person wieder. Damit ist diese Person ein „Diktator“.  $\square$

28. März und 11. April 2014

## 6 Kryptographie

### 6.1 Einfache Verschlüsselungsverfahren

Schon seit Jahrtausenden haben Menschen das Bedürfnis, sich Nachrichten zu schreiben, die niemand außer der vorgesehene Empfänger lesen kann. Dazu müssen die Nachrichten verschlüsselt werden. Eine einfache Möglichkeit dazu bieten *Substitutionschiffren*. Der Name kommt daher,

dass beim Verschlüsseln jeder Buchstabe durch ein anderes Zeichen substituiert (d. h. ersetzt) wird. Eine Tabelle, die solch eine Übersetzung angibt, könnte beispielsweise so aussehen:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\Delta$	$\top$	$\otimes$	$\odot$	$\bigcirc$	$\sqcup$	$\nabla$	$\square$	$\uparrow$	$\cap$	$\vee$	$\#$	$\times$	$\rightarrow$	$\downarrow$	$\heartsuit$	$\vdash$	$\dagger$	$\leftarrow$	$\wedge$	$\diamond$	$\cup$	$\perp$	$\sqcap$	$\oslash$	$\dashv$

Wir müssen uns dabei keine neuen Zeichen ausdenken, sondern können auch die lateinischen Buchstaben selbst wiederverwenden:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	H	B	D	V	T	S	F	M	N	R	K	X	A	J	W	Y	C	P	I	L	G	E	O	U	Z

Angenommen, wir wollen die Nachricht

Mathe macht Spaß!

verschlüsselt versenden. Dazu wollen wir obige Tabelle verwenden. Wir haben noch ein kleineres Problem: Die Nachricht enthält außer Buchstaben auch noch Leerzeichen und Satzzeichen. Diese wollen wir nicht unverschlüsselt in den Geheimtext übernehmen, da sie jemandem, der die Nachricht abfängt, Hinweise auf den Inhalt der Nachricht liefern können. Darum lassen wir sie einfach weg. Aus demselben Grund verwenden wir einheitlich Großbuchstaben. Statt den Umlauten „Ü“, „Ä“ und „Ö“ schreiben wir „UE“, „AE“ und „OE“ wie im Kreuzworträtsel. Ein scharfes ß wird zu *SS*. Die zu verschlüsselnde Nachricht ist also

MATHEMACHTSPASS

Nun suchen wir für jeden Buchstaben dieser Nachricht in der Tabelle den zugehörigen Buchstaben in der Verschlüsselung und schreiben ihn auf:

XQIFVXQBFIPWQPP

Diesen Geheimtext können wir jetzt verschicken. Der Empfänger der Nachricht benötigt dieselbe Tabelle, um die Nachricht wieder zu dechiffrieren. Diese Tabelle ist der Schlüssel in diesem Verschlüsselungs-Verfahren. Wir müssen ihn in einem geheimen Treffen vor Versenden der Nachricht mit dem Empfänger vereinbaren. Dazu schlägt er die Buchstaben des Geheimtextes nacheinander in der zweiten Zeile der Tabelle nach und schreibt den zugehörigen Buchstaben in der ersten Zeile auf.

**Exkurs.** Das Ziel der *Kryptographie* ist es, Nachrichten für Personen außer dem bestimmten Empfänger unlesbar zu machen. Dagegen will die *Steganographie* die Nachricht selbst verstecken. Personen, an die die Nachricht nicht gerichtet ist, sollen also gar nicht erst merken, dass eine Nachricht versandt wurde! Beispiele der Verwendung von Steganographie sind:

- Schreiben mit Geheimtinte, die unter UV-Licht sichtbar wird
- Verstecken einer Referenz auf eine Bibelstelle in einer Adresse auf einer Postkarte
- Einbetten einer geheimen Botschaft in eine Bilddatei durch geringfügiges Abändern der Farbwerte der einzelnen Pixel

Steganographie und Kryptographie können auch kombiniert werden: Dann erhält man Nachrichten, die vor unerwünschten Augen versteckt sind, und die, selbst wenn sie entdeckt werden, nicht gelesen werden können.

Ein weithin bekanntes Verschlüsselungs-Verfahren wurde von Julius Caesar in einem Buch beschrieben. Es wird daher auch *Caesar-Chiffre* genannt. Es handelt sich dabei um einen Spezialfall der Substitutionschiffren. Die Substitutionstabelle entsteht dabei durch Verschieben des Alphabets in der zweiten Zeile. Folgendes Beispiel zeigt eine Verschiebung um fünf Positionen im Alphabet:

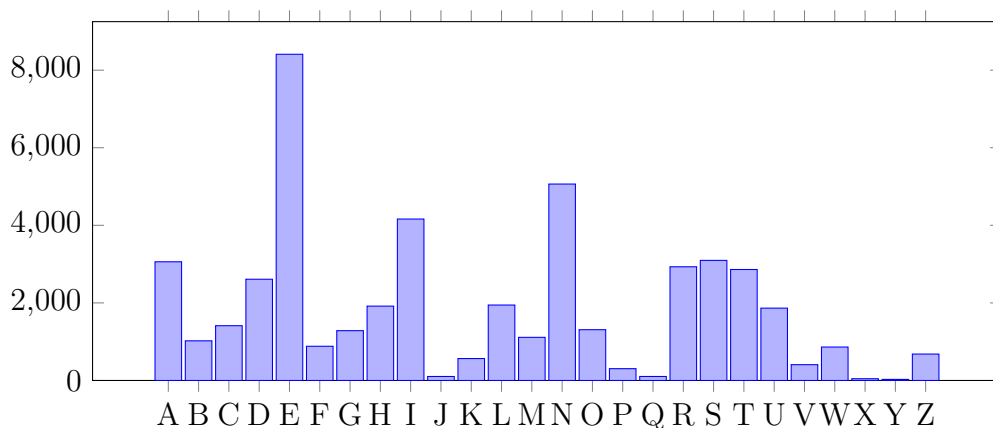
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Da bei obiger Verschiebung das „A“ als „F“ verschlüsselt wird, heißt die obige Verschlüsselung Caesar-Verschlüsselung mit dem Schlüssel „F“. Aus der Information, als welcher Buchstabe das „A“ verschlüsselt wird, kann man leicht herleiten, wie die anderen Buchstaben verschlüsselt werden. Es gibt also 26 verschiedene Möglichkeiten, einen Text mit dem Caesar-Verfahren zu verschlüsseln (den Schlüssel „A“ mit einbezogen, der überhaupt keine Verschlüsselung liefert). Das sind ziemlich wenige Möglichkeiten. Wenn man einen mit diesem Verfahren chiffrierten Text abfängt, so kann man in kurzer Zeit per Hand all diese Möglichkeiten durchgehen und so die Nachricht entschlüsseln. Diesen Ansatz, einfach alle Schlüssel durchzuprobieren, nennt man Brute-Force-Angriff.

Wie viele Tabellen, also mögliche Schlüssel gibt es bei einem allgemeinen Substitutionschiffre? Nun, es gibt 26 verschiedene Möglichkeiten, wie das „A“ verschlüsselt sein kann. Für das „B“ bleiben dann noch 25 mögliche Buchstaben, für das „C“ noch 24 Buchstaben und so weiter. Insgesamt haben wir daher

$$26! = 26 \cdot 25 \cdot \dots \cdot 3 \cdot 2 \cdot 1$$

Möglichkeiten, eine Tabelle zu erstellen. Das sind viel zu viele, um alle auszuprobieren. Darum müssen wir uns einen anderen Ansatz überlegen. Wir nehmen mal an, dass der verschlüsselte Text in Deutsch geschrieben ist. Nun kommen im Deutschen nicht alle Buchstaben gleich häufig vor. Der Vokal „E“ und die Konsonanten „S“ und „N“ kommen beispielsweise sehr oft, die Buchstaben „Q“ und „Y“ sehr selten vor. Das ist auch der Grund, warum es beim Scrabble für den Buchstaben „X“ viel mehr Punkte als für den Buchstaben „E“ gibt. Im nächsten Diagramm siehst du eine Aufschlüsselung dieses Skriptes bis zum Ende dieses Satzes nach Buchstaben:



Bei einem längeren Text lässt dies Rückschlüsse auf die Chiffrierungs-Tabelle zu. Wenn beispielsweise der Buchstabe „W“ in einem Geheimtext häufig vorkommt, so liegt es nahe, dass im Klartext dort überall ein „E“ stand.

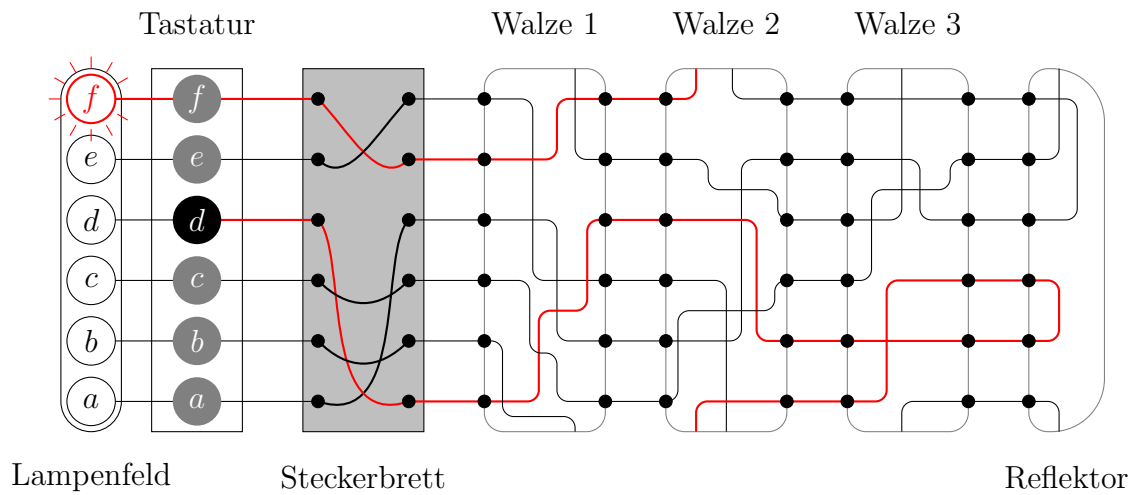
Was ebenfalls helfen kann, sind Buchstabenpaare oder Buchstabentripel, die zusammen vorkommen. Falls in einem Geheimtext häufig „ZWS“ steht, dann könnte es sich dabei um die Verschlüsselung des Artikels „DER“ handeln. Wenn man ein paar Buchstaben auf diese Weise geraten hat, so kann man häufig schon ganze Wörter erkennen und auch die restlichen, weniger häufigen Buchstaben herausfinden. In der Regel schafft man es auf diese Weise, den Geheimtext zu knacken, wenn es sich dabei um einen längeren Text handelt. Bei einem kurzen Text hat man natürlich weniger Anhaltspunkte und muss noch viel mehr rumprobieren.

Ein weiteres Verschlüsselungsverfahren ist der *Vigenère-Chiffre*. Dabei gibt es als Schlüssel ein ganzes Wort, z. B. „KATZE“. Bei der Verschlüsselung gehen wir dann gleichzeitig das Schlüsselwort und den Klartext Buchstabe für Buchstabe durch und verschlüsseln dabei den Buchstaben des Klartextes mit dem Buchstaben des Schlüsselwortes mittels Caesar-Verschiebung. Wenn man am Ende des Schlüsselwortes angelangt ist, startet man einen neuen Durchlauf durch das Schlüsselwort. Durch dieses Verfahren wird das Problem gemindert, dass jedes „E“ im Klartext zu demselben Buchstaben im Geheimtext wird, da die Verschlüsselung nicht nur vom Buchstaben, sondern auch von dessen Position im Text abhängig ist. Folgender Text wurde mit dem Vigenère-Verfahren verschlüsselt:

NIXQSDOKDRICGCHBEAAEBUGCHBEADRCIVGEOHGKMMHPHILEBDMXEFLIMHTMCCADRUENQOTXQDKEAKIBNTBLTEWDQDALSIXDKT  
GUSHCECSLHGRDTRKOHXHQSVGPCSXKEVPAZFOTGZGRJXCIBWNBLCCTAIXAXMHORMTRNMBSHORXMMQMTDMXEINPIAEOLKBXSMCCA  
DZORLVLVUXRWOLNMKQELBLKFYDRGIKCHKBXHHBEASWSCACIBEKRXORHSSBANBLKLLRGRNXPORKNXYRUDDOIVGROTCDHOSFZPGA  
XGVONWRMMHWDVWIMSPORXQSDOKDVCTXHRONLBLBIMSAOIMDVLEPKDWMRNEKDVCTXQSDOKDMXEONPVENLHBEATRQGXLEMHMGED  
AGZPYGUDAOGMRMMHWDVVMYXORHSSBANBLKLLHRXEKDVBOBNVLESDDMHGDXORLSISNXMMHKKHDXHXORPDRDXQSTMTKIBENX  
YRXHROKHLTVEMSIEMWQIRUGFLSNMDVCIVGKOBKZGRTAZXNUKBLNIXRICPKHRJIIDVQIUSWSCADMEZQSOPXQMYDXCLNIXLECCAH  
ROBXEMXDXSNSCADVCTGZGRSXGVVAGFIBZXHXGIXCIBIGHLBEFZYCGTMKCNZRXKNWCMOSMDPVUGFHORJHEEMIXWTKDONBRXEEU  
DVOIGRMMHMEIXSMDVYBXQLKUCICLTLTONYDPNELDVCIVGXVIGMWXKXGREFDMXBNBLCTTAIYDXQISNXYPFXQHSETTJNEKVEVZ  
XZRQEUQEMHMRMXDNDFORWHIKMTIVLXOSCIMHSXANROENYSKOBXMASELBYNXQAKEAMXCIGCHSEPZPJEGCVOHUZVENWJSONGDRW  
IMSIVSKHROSLIVLKZHOSDPMPHXRZYNZQSOEKDQKULLEOILSEVSWDVOIZDRDLBLOWTKDONDNIBPXQYXDWTVMHLBLVIMYISMZDL  
KENRIBAZSZORLSIVLMVIBDXM

Bei obigem Text stellen wir etwas fest: Bestimmte Kombinationen von Buchstaben kommen mehrfach im Text vor. Wir können die Abstände zwischen den Vorkommen der Kombinationen zählen. Beispielsweise liegen zwischen dem Anfang des ersten Vorkommen der Kombination „NIX“ und dem Anfang des zweiten Vorkommen genau 545 Buchstaben. Zwischen dem zweiten und dem dritten Vorkommen liegen 40 Buchstaben. Für das Buchstabentripel „DMX“ sind die Abstände von einem Auftreten zum nächsten: 130, 190, 200 und 185. Was auffällt, ist, dass all diese Zahlen durch 5 teilbar sind (genauer gesagt ist 5 der größte gemeinsame Teiler dieser Zahlen). Und das ist kein Zufall! Diese Buchstabenkombinationen sind höchstwahrscheinlich dadurch entstanden, dass das gleiche Wort verschlüsselt wurde und zufällig beim Verschlüsseln wir uns auch im Schlüsselwort jedes Mal an der gleichen Stelle befunden haben. Damit dies möglich ist, muss das Schlüsselwort genau 5 Buchstaben lang sein. Diese Information hilft uns enorm weiter. Wir wissen nun, dass der 1., der 6., der 11., der 16. und der 21. Buchstabe (usw.) mit derselben Verschiebung Caesar-verschlüsselt wurden. Die genaue Verschiebung können wir mit einer Häufigkeitsanalyse ermitteln. Dazu zählen wir einfach die Vorkommen der Buchstaben an den oben genannten Positionen, malen ein Balkendiagramm wie oben und vergleichen es mit dem Balkendiagramm, dass eine typische Buchstabenverteilung in einem deutschen Text zeigt. So können wir die Verschiebung und damit den ersten Buchstaben des Vigenère-Schlüssels ermitteln. Um die weiteren vier Buchstaben zu ermitteln, gehen wir genauso vor.

## 6.2 Die Entschlüsselung der Enigma



## 6.3 Der Diffie-Hellman-Schlüsselaustausch